COMISSÃO
EUROPEIA

Bruxelas, 25.7.2022
COM(2022) 364 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

Primeiro relatório sobre a aplicação e o funcionamento da Diretiva (UE) 2016/680 relativa à proteção de dados na aplicação da lei («Diretiva Proteção de Dados na Aplicação da Lei»)

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

Primeiro relatório sobre a aplicação e o funcionamento da Diretiva (UE) 2016/680 relativa à proteção de dados na aplicação da lei («Diretiva Proteção de Dados na Aplicação da Lei»)

Índice

1 A Diretiva Proteção de Dados na Aplicação da Lei como principal instrumento para garantir a proteção de dados na política de segurança da União Europeia 3

1.1 Um elemento fundamental de um quadro coerente da União Europeia em matéria de proteção de dados 3

1.2 Um contributo essencial para garantir a robustez da política de segurança na União Europeia 6

1.3 Considerações importantes sobre a elaboração do relatório 7

2 A transposição foi satisfatória, mas subsistem algumas questões 9

2.1 Uma transposição completa, em geral, mas com alguns problemas relativamente a disposições específicas 9

2.2 Prioridades para a avaliação da conformidade 10

2.2.1 Âmbito de aplicação da Diretiva Proteção de Dados na Aplicação da Lei 11

2.2.2 Governação e poderes das autoridades de controlo da proteção de dados 13

2.2.3 Vias de recurso 14

2.2.4 Prazos para a conservação e avaliação 15

2.2.5 Base jurídica do tratamento, incluindo categorias especiais de dados pessoais 16

2.2.6 Decisões automatizadas 17

2.2.7 Direitos dos titulares dos dados 17

2.2.8 Algumas disposições importantes específicas da Diretiva Proteção de Dados na Aplicação da Lei 18

3 Primeiros ensinamentos da aplicação e do funcionamento da Diretiva Proteção de Dados na Aplicação da Lei 19

3.1 Reclamações e impacto positivo nos direitos dos titulares dos dados 19

3.2 Maior sensibilização das autoridades competentes para a proteção de dados 21

3.3 Maior segurança dos dados, mas divergências nas notificações de violação de dados . 22

3.4 Supervisão pelas autoridades de controlo da proteção de dados 24

3.4.1 Recursos das autoridades de controlo da proteção de dados 24

3.4.2 Utilização dos poderes 25

3.4.3 Controlo jurisdicional das ações das autoridades de controlo da proteção de dados 27
3.4.4 Orientações do CEPD 27
3.4.5 Assistência mútua 29
3.5 Instrumento flexível para as transferências internacionais de dados 29
3.5.1 Decisões de adequação 30
3.5.2 Garantias adequadas..... 31
3.5.3 Utilização de derrogações 37
3.5.4 Cooperação policial e judiciária eficaz transnacional..... 37
4 Ações futuras 39

1 A DIRETIVA PROTEÇÃO DE DADOS NA APLICAÇÃO DA LEI COMO PRINCIPAL INSTRUMENTO PARA GARANTIR A PROTEÇÃO DE DADOS NA POLÍTICA DE SEGURANÇA DA UNIÃO EUROPEIA

A presente comunicação apresenta o primeiro relatório da Comissão Europeia sobre a avaliação e revisão da Diretiva (UE) 2016/680[1] relativa à proteção de dados na aplicação da lei («Diretiva Proteção de Dados na Aplicação da Lei»), nos termos do artigo 62.º, n.º 1, da referida diretiva.

O relatório examina, em especial, a aplicação e o funcionamento das regras da Diretiva Proteção de Dados na Aplicação da Lei sobre a transferência de dados pessoais para países terceiros e organizações internacionais, conforme exigido pela referida diretiva, mas adota também uma abordagem mais ampla. Enquadra a Diretiva Proteção de Dados na Aplicação da Lei no direito da UE em matéria de proteção de dados pessoais e no direito da UE que regula o tratamento de dados pessoais para efeitos de prevenção, investigação, deteção ou repressão de infrações penais e execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública («aplicação do direito penal»)[2]. O relatório apresenta uma panorâmica da transposição da Diretiva Proteção de Dados na Aplicação da Lei pelos Estados-Membros para as respetivas legislações nacionais, expõe os primeiros ensinamentos retirados da aplicação e do funcionamento da referida diretiva e descreve o caminho a seguir.

1.1 Um elemento fundamental de um quadro coerente da União Europeia em matéria de proteção de dados

A Diretiva Proteção de Dados na Aplicação da Lei é um dos três pilares do quadro da UE que garante o direito fundamental à proteção dos dados pessoais. Os outros dois são o Regulamento Geral sobre a Proteção de Dados («RGPD»)[3] e o Regulamento relativo à proteção de dados aplicável às instituições e aos órgãos da UE («RPDUE»)[4]. O direito fundamental à proteção de dados está consagrado no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia («Carta»)[5] e no artigo 16.º do Tratado sobre o Funcionamento da União Europeia («TFUE»)[6].

---

[1] Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO L 119 de 4.5.2016, p. 89).

[2] Artigo 1.º, n.º 1, da Diretiva Proteção de Dados na Aplicação da Lei.

[3] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (JO L 119 de 4.5.2016, p. 1).

[4] Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

[5] Carta dos Direitos Fundamentais da União Europeia (JO C 202 de 7.6.2016, p. 389).

[6] Versão consolidada do Tratado sobre o Funcionamento da União Europeia (JO C 202 de 7.6.2016, p. 47).

A Diretiva Proteção de Dados na Aplicação da Lei entrou em vigor em 6 de maio de 2016 e os Estados-Membros tinham de a transpor até 6 de maio de 2018[7].

A Diretiva Proteção de Dados na Aplicação da Lei é o primeiro ato legislativo da UE que adota uma abordagem global da proteção de dados pessoais pelas autoridades competentes (ou seja, autoridades judiciais, policiais e outras autoridades responsáveis pela aplicação do direito penal, conforme previsto no artigo 3.º, ponto 7, da referida diretiva) para efeitos de aplicação do direito penal. Em comparação com a Decisão-Quadro 2008/977/JHA do Conselho[8], que revogou e substituiu, a Diretiva Proteção de Dados na Aplicação da Lei constitui um avanço importante para assegurar a aplicação coerente das regras relativas à proteção de dados em toda a UE. Em primeiro lugar, a Diretiva Proteção de Dados na Aplicação da Lei prevê um conjunto completo de regras para o tratamento transfronteiriço e nacional de dados pessoais para efeitos de aplicação do direito penal, ao passo que a decisão-quadro do Conselho abrange apenas o tratamento transfronteiriço. Em segundo lugar, a Diretiva Proteção de Dados na Aplicação da Lei prevê um conjunto de regras abrangente e horizontal, ao passo que, segundo a abordagem anterior, cada ato setorial da UE que previa o tratamento de dados pessoais no contexto da aplicação do direito penal era regido pelas suas próprias regras em matéria de proteção de dados[9].

O RGPD, o RPDUE e a Diretiva Proteção de Dados na Aplicação da Lei baseiam-se em conceitos e princípios semelhantes[10], o que resulta numa interpretação e aplicação coerentes das regras da UE em matéria de proteção de dados. Estes atos partilham definições comuns e contêm obrigações semelhantes para os responsáveis pelo tratamento de dados e os subcontratantes. Contudo, a Diretiva Proteção de Dados na Aplicação da Lei também aborda especificamente os riscos associados ao tratamento de dados pessoais no contexto da aplicação do direito penal. As disposições correspondentes incluem obrigações de i) distinguir entre diferentes categorias de titulares de dados, ii) distinguir entre dados pessoais baseados em factos e dados baseados numa avaliação pessoal, iii) manter um registo da utilização de dados pessoais e cumprir requisitos de segurança específicos[11].

Dada a natureza específica da cooperação judiciária em matéria penal e da cooperação policial, considerou-se necessário adotar regras específicas nestes domínios para a proteção dos dados pessoais e a livre circulação de dados pessoais[12]. A natureza sensível do domínio da cooperação

---

[7] Artigo 63.º, n.º 1, da Diretiva Proteção de Dados na Aplicação da Lei.

[8] Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (JO L 350 de 30.12.2008, p. 60).

[9] Por exemplo, os atos jurídicos que regulam o Sistema de Informação Schengen e outros instrumentos do acervo de Schengen continham disposições específicas que regulavam questões como os direitos dos titulares dos dados.

[10] Estes incluem a licitude e a lealdade; a limitação da finalidade; a minimização dos dados; a exatidão; a limitação da conservação; a integridade e confidencialidade; e a responsabilização (artigo 4.º da Diretiva Proteção de Dados na Aplicação da Lei).

[11] Artigos 6.º, 7.º, 25.º e 29.º da Diretiva Proteção de Dados na Aplicação da Lei, respetivamente.

[12] Declaração n.º 21 sobre a proteção de dados pessoais no domínio da cooperação judiciária em matéria penal e da cooperação policial — anexada à Ata Final da Conferência Intergovernamental que aprovou o Tratado de Lisboa (JO C 115 de 9.5.2008, p. 345).

judiciária em matéria penal e da cooperação policial, juntamente com a complexidade dos quadros jurídicos nacionais que regulam a aplicação do direito penal, levou a que se considerasse que uma diretiva seria o melhor instrumento para alcançar um elevado nível de proteção de dados neste domínio. Uma diretiva também proporciona aos Estados-Membros a flexibilidade necessária na aplicação dos princípios, regras e isenções a nível nacional[13].

A Comissão publicou o seu primeiro relatório sobre a aplicação do RGPD em 24 de junho de 2020[14]. Concluiu que, de um modo geral, o RGPD cumpria os seus objetivos, nomeadamente proporcionando aos cidadãos um conjunto sólido de direitos oponíveis e criando um novo sistema de governação e execução da UE. O relatório estabelece uma lista de medidas a tomar para facilitar ainda mais a aplicação do RGPD por todas as partes interessadas e para promover e continuar a desenvolver uma cultura de proteção de dados na UE, a par de uma aplicação rigorosa.

O presente relatório surge na sequência da revisão dos atos jurídicos adotados pela UE que regulam o tratamento de dados pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais. O objetivo dessa revisão era avaliar a necessidade de alinhar os atos jurídicos em causa com a Diretiva Proteção de Dados na Aplicação da Lei[15]. Em 24 de junho de 2020, a Comissão cumpriu essa obrigação ao adotar uma comunicação intitulada «Ações futuras para alinhar o acervo do antigo terceiro pilar com as regras de proteção de dados»[16]. Identificou dez atos jurídicos que devem ser alinhados com a Diretiva Proteção de Dados na Aplicação da Lei e estabeleceu um calendário para este trabalho.

Por último, o presente relatório foi elaborado em paralelo com o relatório da Comissão sobre a aplicação do RPDUE. Um elemento importante desta última é a revisão das suas regras, estabelecidas no capítulo IX, relativas ao tratamento de dados pessoais operacionais pelos órgãos e organismos da UE no exercício de atividades abrangidas pelo âmbito da cooperação policial e da cooperação judiciária em matéria penal[17] («organismos JAI»). As regras em causa baseiam-se, em grande medida, na Diretiva Proteção de Dados na Aplicação da Lei. Nos termos do artigo 98.º do RPDUE, a Comissão deve reexaminar os atos jurídicos que regulam o tratamento de dados pessoais operacionais pelos organismos JAI e pode apresentar propostas legislativas adequadas,

---

[13] Exposição de motivos da proposta de diretiva relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados, COM(2012) 10 final de 25 de janeiro de 2012.

[14] Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «A proteção de dados enquanto pilar da capacitação dos cidadãos e a abordagem da UE para a transição digital — dois anos de aplicação do Regulamento Geral sobre a Proteção de Dados», COM(2020) 264 final de 24 de junho de 2020.

[15] Nos termos do artigo 62.º, n.º 6, da Diretiva Proteção de Dados na Aplicação da Lei, a Comissão deve reexaminar, até 6 de maio de 2019, outros atos jurídicos adotados pela UE que regulam o tratamento de dados pessoais para efeitos de aplicação da lei, a fim de avaliar a necessidade de os harmonizar com a Diretiva Proteção de Dados na Aplicação da Lei e, se for caso disso, propor alterações a esses outros atos jurídicos da UE de forma a assegurar uma abordagem coerente da proteção de dados pessoais no âmbito da Diretiva Proteção de Dados na Aplicação da Lei.

[16] Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Ações futuras para alinhar o acervo do antigo terceiro pilar com as regras de proteção de dados», COM(2020) 262 final de 24 de junho de 2020.

[17] Parte III, título V, capítulos 4 e 5, do TFUE.

nomeadamente na perspetiva da aplicação das regras do capítulo IX, à Europol[18] e à Procuradoria Europeia, bem como propor quaisquer adaptações necessárias ao referido capítulo.

1.2 Um contributo essencial para garantir a robustez da política de segurança na União Europeia

A Comissão tem repetidamente salientado que uma UE eficaz e verdadeiramente segura só pode ser construída com base no pleno respeito dos direitos fundamentais consagrados na Carta e no direito derivado da UE. A Diretiva Proteção de Dados na Aplicação da Lei contribui de forma decisiva para a política de segurança da UE, assegurando que os dados pessoais das vítimas, das testemunhas e dos suspeitos de crimes são devidamente protegidos. Além disso, ao harmonizar as regras em matéria de proteção dos dados pessoais tratados pelas autoridades competentes dos países da UE e de Schengen, a Diretiva Proteção de Dados na Aplicação da Lei contribui para aumentar a confiança e a segurança dos dados trocados entre as autoridades para efeitos de aplicação do direito penal, facilitando assim a cooperação transfronteiriça na luta contra a criminalidade e o terrorismo[19]. A Diretiva Proteção de Dados na Aplicação da Lei também desempenha um papel fundamental na promoção de uma cultura de conformidade em matéria de proteção de dados entre as autoridades competentes.

A Estratégia para a União da Segurança[20] salienta ainda que as novas tecnologias, como a inteligência artificial, podem ser utilizadas como um instrumento poderoso para combater a criminalidade. A realização deste potencial implica também garantir os mais exigentes padrões de cumprimento dos direitos fundamentais. A legislação em matéria de proteção de dados, nomeadamente a Diretiva Proteção de Dados na Aplicação da Lei, constitui a base para a elaboração de legislação setorial. Por exemplo, a proposta de Regulamento Inteligência Artificial[21] enquadraria melhor a utilização de dados pessoais para identificação biométrica à distância em locais públicos para efeitos de aplicação da lei.

Por último, num mundo interligado, a criminalidade (e a cibercriminalidade e outra criminalidade possibilitada pelo ciberespaço, em particular) são cada vez mais de natureza transfronteiriça. Mesmo quando investigam casos nacionais, as autoridades competentes cada vez mais se deparam com situações transfronteiriças porque as informações são armazenadas eletronicamente num país terceiro. Esta situação aumenta a necessidade de cooperação internacional no domínio das investigações penais, tanto por parte das autoridades dos Estados-Membros como por parte de

[18] Esta questão já foi abordada na proposta da Comissão de 2020 que altera o Regulamento Europol.
[19] Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Primeiro relatório intercalar sobre a Estratégia da UE para a União da Segurança», COM(2020 797 final de 9 de dezembro de 2020.
[20] Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre a Estratégia da UE para a União da Segurança, COM(2020) 605 final de 24 de julho de 2020.
[21] Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União, COM(2021) 206 final de 21 de abril de 2021.

organismos da UE como a Europol e a Eurojust. Essa cooperação, em especial a recolha e o intercâmbio de provas eletrónicas[22], envolve frequentemente a transferência de dados pessoais. Por conseguinte, são essenciais salvaguardas sólidas em matéria de proteção de dados, as quais contribuem igualmente para aumentar a confiança entre as autoridades responsáveis pela aplicação da lei, assegurando um intercâmbio de informações mais rápido e eficaz e reforçando a segurança jurídica quando as informações são posteriormente utilizadas em processos penais. A este respeito, a Diretiva Proteção de Dados na Aplicação da Lei prevê um conjunto atualizado de instrumentos para facilitar essas transferências de dados pessoais da UE para um país terceiro ou uma organização internacional (por exemplo, a Interpol[23]), assegurando simultaneamente que os dados pessoais continuam a beneficiar de um elevado nível de proteção. A Comissão e os Estados-Membros recorreram a toda a gama de instrumentos da Diretiva Proteção de Dados na Aplicação da Lei desde a sua entrada em vigor, confirmando assim que esta é suficientemente ampla e flexível para permitir uma cooperação policial e judiciária internacional eficaz.

1.3 Considerações importantes sobre a elaboração do relatório

Ao preparar o presente relatório, a Comissão reuniu informações e comentários provenientes de diversas fontes e de atividades de consulta específicas. Nos termos do artigo 62.º da Diretiva Proteção de Dados na Aplicação da Lei, a Comissão teve em conta os contributos e as posições do Parlamento Europeu[24], do Conselho[25], do Comité Europeu para a Proteção de Dados («CEPD»)[26] e das autoridades nacionais de controlo da proteção de dados. Foi possível recolher mais opiniões através de um questionário dirigido às organizações da sociedade civil (através da Agência dos

[22] As informações e os elementos de prova eletrónicos são necessários em cerca de 85 % das investigações relativas a crimes graves, enquanto 65 % do total dos pedidos se destina a prestadores estabelecidos noutra jurisdição. Ver o Documento de trabalho dos serviços da Comissão intitulado «Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings» (não traduzido para português), SWD(2018) 118 final.

[23] Ver também o considerando 25 da Diretiva Proteção de Dados na Aplicação da Lei.

[24] Contributo da Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos do Parlamento Europeu para o próximo relatório da Comissão Europeia sobre a avaliação e revisão da Diretiva Proteção de Dados na Aplicação da Lei, 7 de fevereiro de 2022.

[25] Posição do Conselho e conclusões sobre a aplicação da Diretiva Proteção de Dados na Aplicação da Lei (documento do Conselho 13943/21 de 18 de novembro de 2021 https://www.consilium.europa.eu/media/54304/st_13943_2021_init_en.pdf).

[26] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei pela Comissão Europeia nos termos do artigo 62.º da referida diretiva, adotada em 14 de dezembro de 2021 («contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei»). https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf.

Direitos Fundamentais da União Europeia)[27] e das respostas a um convite público à apreciação[28]. A Comissão teve igualmente em consideração as observações do Grupo de Peritos dos Estados-Membros sobre o RGPD e a Diretiva Proteção de Dados na Aplicação da Lei[29], bem como as observações da Presidência alemã do Conselho[30]. Teve igualmente em conta a análise das medidas nacionais de transposição e um pequeno número de reclamações recebidas a este respeito.

Embora a Diretiva Proteção de Dados na Aplicação da Lei seja aplicável a todos os Estados-Membros e a todos os países Schengen (porque constitui um desenvolvimento do acervo de Schengen[31]), o presente relatório abrange apenas os Estados-Membros da UE.

Houve três fatores que afetaram a elaboração do presente relatório. Em primeiro lugar, dois terços dos Estados-Membros não cumpriram o prazo de maio de 2018 para a transposição da Diretiva Proteção de Dados na Aplicação da Lei para o direito nacional. Não obstante, a maioria dos Estados-Membros transpôs a Diretiva Proteção de Dados na Aplicação da Lei até 2019, após a Comissão ter dado início a procedimentos de infração. Por conseguinte, a experiência em relação à sua aplicação é bastante limitada, aspeto que o CEPD[32] e o Conselho[33] também sublinham. Em segundo lugar, revelou-se mais difícil compilar estatísticas sobre a aplicação da Diretiva Proteção de Dados na Aplicação da Lei, em comparação com o RGPD. Algumas autoridades de controlo da proteção de dados não recolhem estatísticas sobre as suas atividades de controlo separadamente para a Diretiva Proteção de Dados na Aplicação da Lei e o RGPD. É o caso, por exemplo, das notificações de violação de dados[34] e das reclamações apresentadas ao abrigo da Diretiva Proteção de Dados na Aplicação da Lei[35], o que, por vezes, dificulta a obtenção de uma visão exata destas disposições ao abrigo da referida diretiva[36].

---

[27] Das 804 organizações da sociedade civil contactadas pela Agência dos Direitos Fundamentais da União Europeia (FRA), 88 responderam. Contudo, apenas foi possível considerar *17 dos contributos, devido ao facto de 61 contributos não estarem relacionados com a Diretiva Proteção de Dados na Aplicação da Lei* ou de indicarem que a organização em causa não trabalha na proteção dos direitos fundamentais no domínio da aplicação do direito penal ou não *está* de todo familiarizada com a diretiva.

[28] Convite à apreciação, Proteção de dados na aplicação da lei — relatório acerca da Diretiva sobre a Proteção de Dados na Aplicação da Lei, 24 de janeiro de 2022. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13288-Data-protection-in-law-enforcement-report-on-the-Law-Enforcement-Directive_pt.

[29] Grupo de peritos da Comissão sobre o Regulamento (UE) 2016/679 e a Diretiva (UE) 2016/680 (E03461); https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3461.

[30] Relatório da Presidência do Conselho da União Europeia sobre o intercâmbio de dados policiais com países terceiros — Experiências na aplicação do artigo 37.º da Diretiva Proteção de Dados na Aplicação da Lei, dezembro de 2020.

[31] Ver os considerandos 101 a 103 da Diretiva Proteção de Dados na Aplicação da Lei.

[32] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 4.

[33] Posição do Conselho e conclusões sobre a aplicação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 7.

[34] Por exemplo, as autoridades da Dinamarca, Lituânia, Noruega, Áustria e várias autoridades da Alemanha não dispõem de estatísticas separadas sobre violações de dados ao abrigo da Diretiva Proteção de Dados na Aplicação da Lei. Seis autoridades comunicaram igualmente que não receberam notificações de violação de dados ao abrigo da Diretiva Proteção de Dados na Aplicação da Lei.

[35] Por exemplo, as autoridades da Dinamarca e da Áustria e várias autoridades da Alemanha não dispõem de estatísticas separadas para as reclamações apresentadas ao abrigo da Diretiva Proteção de Dados na Aplicação da Lei.

[36] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 43.

Em terceiro lugar, é importante considerar que o desenvolvimento da jurisprudência no que diz respeito à aplicação da Diretiva Proteção de Dados na Aplicação da Lei ainda está numa fase inicial. Atualmente, estão pendentes no Tribunal de Justiça da União Europeia («TJUE») vários processos relativos à interpretação de disposições fundamentais da Diretiva Proteção de Dados na Aplicação da Lei, designadamente o direito de acesso dos titulares dos dados e o direito a intentar ação judicial. Estes acórdãos proporcionarão maior clareza e contribuirão para uma abordagem mais harmonizada entre os Estados-Membros.

2 A TRANSPOSIÇÃO FOI SATISFATÓRIA, MAS SUBSISTEM ALGUMAS QUESTÕES

A Comissão criou um grupo de peritos dos Estados-Membros[37], para os ajudar a incorporar a Diretiva Proteção de Dados na Aplicação da Lei no direito nacional, o qual facilita os debates e a partilha de experiências entre os Estados-Membros e a Comissão sobre as regras em matéria de proteção de dados. Este grupo reuniu-se regularmente entre a adoção da Diretiva Proteção de Dados na Aplicação da Lei, em 2016, e o prazo de transposição de maio de 2018, tendo os seus trabalhos sido retomados em 2021.

A panorâmica da transposição a seguir apresentada centra-se nas principais questões identificadas até à data. Baseia-se principalmente na análise pela Comissão das informações fornecidas pelos Estados-Membros aquando da notificação à Comissão das medidas nacionais que tomaram para transpor a Diretiva Proteção de Dados na Aplicação da Lei para o direito nacional. Esta análise foi apoiada por um estudo externo, realizado por um contratante externo. A Comissão encetou igualmente intercâmbios bilaterais com vários Estados-Membros.

2.1 Uma transposição completa, em geral, mas com alguns problemas relativamente a disposições específicas

Em julho de 2018, a Comissão deu início a procedimentos de infração contra 19 Estados-Membros por não terem adotado legislação de transposição da Diretiva Proteção de Dados na Aplicação da Lei até maio de 2018 e por não terem notificado devidamente a Comissão da sua transposição. Em julho de 2019, foi foi dado início a outro procedimento contra outro Estado-Membro por não transposição parcial. Consequentemente, a maioria dos Estados-Membros notificou posteriormente a Comissão da sua legislação nacional de transposição, tendo esta última encerrado gradualmente os procedimentos de infração contra eles instaurados em 2019 (em 2020, no caso de um Estado-Membro). Em 2021, a Comissão instaurou uma ação por incumprimento no TJUE contra a Espanha, uma vez que esta ainda não tinha transposto a Diretiva Proteção de Dados na Aplicação da Lei nem notificado a Comissão das suas medidas de transposição. Tendo em conta a gravidade e a duração da infração, o TJUE, pela primeira vez, condenou a Espanha ao pagamento de uma quantia fixa e de uma sanção pecuniária compulsória[38].

[37] Ver nota de rodapé 29.

[38] Acórdão do Tribunal de Justiça de 25 de fevereiro de 2021, Comissão Europeia/Reino de Espanha, C-658/19, ECLI:EU:C:2017:548.

A Comissão lançou igualmente, em abril de 2022, um procedimento de infração contra a Alemanha, após ter detetado uma lacuna na transposição da Diretiva Proteção de Dados na Aplicação da Lei em relação às atividades da Polícia Federal alemã.

A Comissão continuará a avaliar a transposição da Diretiva Proteção de Dados na Aplicação da Lei nos Estados-Membros e tomará as medidas necessárias para colmatar eventuais lacunas.

2.2 Prioridades para a avaliação da conformidade

A Comissão está igualmente a verificar se as disposições nacionais dos Estados-Membros transpuseram corretamente os requisitos da Diretiva Proteção de Dados na Aplicação da Lei (verificação da conformidade).

Ao transporem a referida diretiva, os Estados-Membros alteraram a sua legislação anterior em matéria de proteção de dados ou revogaram-na e substituíram-na por um novo(s) ato(s) horizontal(ais) de proteção de dados. Em muitos casos, a legislação nacional transpõe a Diretiva Proteção de Dados na Aplicação da Lei remetendo para a mesma disposição ou disposição equivalente do RGPD (por exemplo, no que diz respeito às definições, às notificações de violações de dados, à nomeação do encarregado da proteção de dados e às disposições sobre a organização, o estatuto, as competências, as atribuições e os poderes das autoridades nacionais de controlo da proteção de dados). Algumas das disposições da Diretiva Proteção de Dados na Aplicação da Lei foram também transpostas através de novas disposições, por exemplo, no direito administrativo geral, no direito processual administrativo ou no processo penal. Alguns Estados-Membros também transpuseram uma série de disposições da Diretiva Proteção de Dados na Aplicação da Lei para a legislação setorial que regula o funcionamento e os poderes de autoridades competentes específicas. Por conseguinte, pode ser necessário ter em conta vários atos jurídicos nacionais para determinar se a diretiva foi ou não corretamente transposta num determinado Estado-Membro. De um modo geral, as legislações nacionais refletem em grande medida os princípios e as disposições fundamentais da Diretiva Proteção de Dados na Aplicação da Lei. Contudo, foram identificadas várias questões, as mais importantes das quais são descritas nas secções seguintes. A Comissão já deu início a vários procedimentos de infração contra Estados-Membros[39]. O processo de revisão continua em curso e a Comissão continuará a utilizar todos os instrumentos disponíveis,

[39] Em abril de 2022, a Comissão deu início a procedimentos de infração contra a Grécia, a Finlândia e a Suécia, alegando que as respetivas legislações nacionais de transposição não estão em conformidade com a Diretiva Proteção de Dados na Aplicação da Lei. O processo contra a Grécia diz respeito a *uma série de pontos, incluindo, nomeadamente*, a não aplicação da legislação nacional que transpõe a Diretiva Proteção de Dados na Aplicação da Lei ao tratamento de dados pessoais pelas autoridades judiciais e pelas autoridades que atuam sob a sua supervisão para a maioria das infrações penais; a transposição das disposições em matéria de armazenamento e revisão de dados (artigo 5.º); a base jurídica do tratamento de dados (artigo 8.º); e salvaguardas no contexto das decisões automatizadas (artigo 11.º). Os procedimentos de infração contra a Finlândia e a Suécia foram iniciados porque as respetivas leis não proporcionam aos titulares dos dados acesso a uma via de recurso efetiva perante um tribunal. A Comissão deu início a um procedimento de infração contra a Alemanha em maio de 2022, uma vez que várias leis nacionais de transposição da Diretiva Proteção de Dados na Aplicação da Lei não preveem poderes de correção eficazes a nível federal e dos Länder.

nomeadamente infrações, quando uma medida nacional de transposição não estiver em conformidade com a Diretiva Proteção de Dados na Aplicação da Lei.

A jurisprudência sobre a Diretiva Proteção de Dados na Aplicação da Lei ainda está numa fase muito inicial. O TJUE começou a proferir acórdãos sobre a interpretação da Diretiva Proteção de Dados na Aplicação da Lei, nomeadamente *nos* processos WS contra Bundesrepublik Deutschland[40] e B contra Latvijas Republikas Saeima[41]. Aquando da redação do presente relatório, estão pendentes no TJUE várias decisões prejudiciais (como indicado nas secções seguintes).

2.2.1 Âmbito de aplicação da Diretiva Proteção de Dados na Aplicação da Lei

A dificuldade de delimitar o âmbito de aplicação da Diretiva Proteção de Dados na Aplicação da Lei e o âmbito de aplicação do RGPD foi suscitada como uma questão preocupante tanto pelo grupo de peritos dos Estados-Membros sobre o RGPD e a Diretiva Proteção de Dados na Aplicação da Lei[42], como pelo CEPD[43]. Algumas autoridades de controlo da proteção de dados observaram igualmente que as autoridades competentes podem sentir dificuldades neste aspeto[44].

O âmbito de aplicação da Diretiva Proteção de Dados na Aplicação da Lei é definido[45] por dois elementos fundamentais: a noção de autoridade competente (âmbito de aplicação pessoal) e a noção de infração penal (âmbito de aplicação material).

No que diz respeito ao âmbito de aplicação pessoal, o tratamento de dados é abrangido pela Diretiva Proteção de Dados na Aplicação da Lei, em primeiro lugar, quando é efetuado por uma autoridade competente e, em segundo lugar, quando os dados pessoais são tratados para efeitos da referida diretiva[46] (ou seja, para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública). Segundo a Comissão, as «autoridades competentes», conforme definidas pela Diretiva Proteção de Dados na Aplicação da Lei[47], tanto podem ser órgãos do Estado como

---

[40] Acórdão do Tribunal de Justiça de 12 de maio de 2021, Bundesrepublik Deutschland, C-505/19, ECLI:EU:C:2021:376. O processo dizia respeito, entre outras questões, à licitude do tratamento de dados pessoais [artigo 4.º, n.º 1, alínea a), e artigo 8.º da Diretiva Proteção de Dados na Aplicação da Lei] no contexto específico de um alerta vermelho emitido pela Interpol. O Tribunal de Justiça não se opôs a que os dados pessoais constantes de um alerta vermelho emitido pela Interpol fossem tratados como lícitos enquanto não fosse estabelecido, numa decisão judicial transitada em julgado, que o princípio *ne bis in idem* se aplica aos factos em que esse alerta se baseia.

[41] Acórdão do Tribunal de Justiça de 22 de junho de 2021, Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504. O TJUE interpretou a definição de autoridade competente nos termos do artigo 3.º, ponto 7, e o conceito de crime. Ver também a secção *infra*.

[42] Ver a ata da reunião do grupo de peritos da Comissão sobre o Regulamento (UE) 2016/679 e a Diretiva (UE) 2016/680, de 5 de maio de 2021 https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=pt&meetingId=25283&fromExpertGroups=true.

[43] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 7.

[44] As autoridades de controlo da proteção de dados da Irlanda, França e Hungria suscitaram esta questão como uma preocupação.

[45] Artigo 2.º, n.º 1, da Diretiva Proteção de Dados na Aplicação da Lei e considerandos 12 a 14 da mesma diretiva.

[46] Artigo 1.º da Diretiva Proteção de Dados na Aplicação da Lei.

[47] Artigo 3.º, ponto 7, da Diretiva Proteção de Dados na Aplicação da Lei.

organismos privados, aos quais a lei confere poderes especiais para além dos que resultam das regras normais aplicáveis nas relações entre particulares e/ou da possibilidade de exercer o poder coercivo. Estas autoridades são autoridades competentes nos termos da Diretiva Proteção de Dados na Aplicação da Lei quando (ainda que apenas esporadicamente e/ou em casos isolados) tratam dados para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais (incluindo a salvaguarda e a prevenção de ameaças à segurança pública). Tal significa, por exemplo, que o tratamento por esses órgãos de dados pessoais para fins não abrangidos pela Diretiva Proteção de Dados na Aplicação da Lei [por exemplo, recursos humanos ou outros fins administrativos, como o tratamento de dados pessoais pelas Unidades de Informação Financeira (UIF) ao abrigo do acervo em matéria de luta contra o branqueamento de capitais[48]] é abrangido pelo âmbito de aplicação do RGPD e não pelo âmbito de aplicação da Diretiva Proteção de Dados na Aplicação da Lei.

O conceito de «infração penal» é de extrema importância quando se determina se o tratamento de dados é ou não abrangido pelo âmbito de aplicação da Diretiva Proteção de Dados na Aplicação da Lei. De acordo com o TJUE, são pertinentes três critérios para apreciar o caráter penal de uma infração: se a infração é qualificada como penal nos termos do direito nacional, a própria natureza da infração e o grau de severidade da sanção suscetível de ser aplicada ao interessado[49]. O caráter autónomo do conceito de infração penal referido no considerando 13 da Diretiva Proteção de Dados na Aplicação da Lei implica, entre outros, que o direito dos Estados-Membros não possa determinar a natureza de uma infração como sendo «penal» apenas para efeitos da aplicação da Diretiva Proteção de Dados na Aplicação da Lei.

A questão da delimitação dos âmbitos de aplicação do RGPD e da Diretiva Proteção de Dados na Aplicação da Lei surge em alguns Estados-Membros no que diz respeito à delimitação dos domínios das infrações penais e das infrações administrativas. Em especial, algumas legislações nacionais de transposição referem-se a finalidades do tratamento de dados pessoais que não estão enumeradas no artigo 1.º da Diretiva Proteção de Dados na Aplicação da Lei (por exemplo, ameaças à ordem pública ou à segurança pública). A questão também se coloca porque alguns Estados-Membros consideram que vários órgãos administrativos (por exemplo, as UIF, conforme acima referido) desempenham funções abrangidas pela Diretiva Proteção de Dados na Aplicação da Lei.

A legislação dos Estados-Membros, na sua maioria, prevê de forma abrangente as autoridades competentes para o tratamento de dados para efeitos da Diretiva Proteção de Dados na Aplicação da Lei. Em contrapartida, alguns Estados-Membros optaram por enumerar exaustivamente as autoridades competentes nos termos do disposto na Diretiva Proteção de Dados na Aplicação da

---

[48] O artigo 41.º da Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, que altera o Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho, e que revoga a Diretiva 2005/60/CE do Parlamento Europeu e do Conselho e a Diretiva 2006/70/CE da Comissão, que regulamenta o funcionamento das Unidades de Informação Financeira, enuncia explicitamente que o tratamento de dados pessoais ao abrigo dessa diretiva está sujeito ao Regulamento (UE) 2016/679.

[49] Acórdão do Tribunal de Justiça de 22 de junho de 2021, Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021: 504, n.º 87.

Lei na sua legislação nacional. Alguns Estados-Membros também previram uma derrogação para o tratamento por parte de determinados tipos de autoridades competentes ou de determinados tipos de dados.

A questão do âmbito de aplicação da Diretiva Proteção de Dados na Aplicação da Lei é objeto de um pedido de decisão prejudicial no TJUE. O tribunal Landesverwaltungsgericht Tirol (Áustria) levantou a questão do âmbito de aplicação da Diretiva Proteção de Dados na Aplicação da Lei quando uma autoridade competente tentou, sem êxito, aceder a dados num telefone apreendido (interpretação do artigo 2.º da referida diretiva). O processo diz igualmente respeito às condições desse acesso[50].

2.2.2 Governação e poderes das autoridades de controlo da proteção de dados

Todos os Estados-Membros, à exceção de dois (Bélgica e Suécia), confiaram a aplicação da Diretiva Proteção de Dados na Aplicação da Lei à autoridade de controlo que é igualmente responsável pela aplicação do RGPD. A Bélgica confiou a supervisão da polícia para efeitos da Diretiva Proteção de Dados na Aplicação da Lei a uma autoridade de controlo diferente. Na Suécia, a supervisão de determinadas autoridades competentes, nomeadamente a polícia, é partilhada entre a autoridade de controlo responsável pelo RGPD e outra autoridade de controlo. Além disso, nos termos da Diretiva Proteção de Dados na Aplicação da Lei, todas as autoridades de controlo da proteção de dados não têm competência para fiscalizar os tribunais quando atuam no exercício das suas funções jurisdicionais.

No que diz respeito às disposições da Diretiva Proteção de Dados na Aplicação da Lei relativas à independência das autoridades de controlo da proteção de dados[51], todos os Estados-Membros estipularam, na sua legislação de transposição, que as autoridades de controlo da proteção de dados devem agir de forma independente no exercício das suas atribuições. Exigem igualmente que os membros das suas autoridades de controlo da proteção de dados não estejam sujeitos a influências externas e não recebam nem procurem obter instruções de ninguém.

O controlo do cumprimento pelas autoridades de controlo da proteção de dados é crucial e está consagrado no artigo 8.º, n.º 3, da Carta. A Diretiva Proteção de Dados na Aplicação da Lei exige que os Estados-Membros dotem as autoridades de controlo da proteção de dados de poderes de investigação, corretivos e consultivos, que devem ser eficazes. Trata-se de um pré-requisito para a correta aplicação das regras de proteção de dados e, por conseguinte, para a consecução do objetivo da Diretiva Proteção de Dados na Aplicação da Lei de um elevado nível de proteção dos direitos fundamentais, em especial no que diz respeito ao direito à proteção dos dados pessoais, e para garantir a livre circulação de dados na UE. As autoridades de controlo da proteção de dados

[50] Pedido de decisão prejudicial no processo C.G./Bezirkshauptmannschaft Landeck, C-548/21.
[51] Capítulo VI, secção 1, da Diretiva Proteção de Dados na Aplicação da Lei.

devem dispor de poderes equivalentes em toda a UE, para poderem desempenhar as suas atribuições conforme previsto na Diretiva Proteção de Dados na Aplicação da Lei[52].

Todos os Estados-Membros conferiram às suas autoridades os poderes de investigação especificados na Diretiva Proteção de Dados na Aplicação da Lei e a maioria dos Estados-Membros conferiu-lhes igualmente outros poderes (por exemplo, realizar auditorias, entrar em instalações, fazer cópias de dados e apreender objetos[53]). Consequentemente, quase todas as autoridades de controlo da proteção de dados consideraram que dispõem de poderes de investigação eficazes.

Quase todos os Estados-Membros previram os poderes de correção especificados na Diretiva Proteção de Dados na Aplicação da Lei[54]. Muitos fizeram-no seguindo de perto a redação da Diretiva Proteção de Dados na Aplicação da Lei, ao passo que vários utilizaram uma formulação muito ampla, que pode ser razoavelmente interpretada como abrangendo todos os poderes previstos na referida diretiva.

Além disso, a maior parte da legislação dos Estados-Membros confere às autoridades de controlo da proteção de dados o poder de aplicar coimas[55].

Nem todos os Estados-Membros conferiram às suas autoridades de controlo da proteção de dados o poder de levar ao conhecimento das autoridades judiciais as infrações à legislação nacional adotada para transpor a Diretiva Proteção de Dados na Aplicação da Lei e de intentar ou de outro modo intervir em processos judiciais. Este poder é importante e complementa os outros meios à disposição das autoridades de controlo em matéria de proteção de dados para assegurar eficazmente um elevado nível de proteção dos direitos fundamentais das pessoas e, em especial, do direito que têm à proteção dos seus dados pessoais.

2.2.3 Vias de recurso

Todos os Estados-Membros previram o direito de apresentar uma reclamação à sua autoridade de controlo competente[56]. As legislações nacionais, na sua maioria, preveem um prazo para a

---

[52] Considerandos 7 e 82 da Diretiva Proteção de Dados na Aplicação da Lei.

[53] Ver também o n.º 23 do contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei: 24 Estados-Membros previram o poder de obter acesso a quaisquer instalações do responsável pelo tratamento e do subcontratante, bem como a qualquer equipamento e meios de tratamento de dados; 21 Estados-Membros previram um processo de auditoria e nove Estados-Membros previram outros poderes (por exemplo, apreensão de objetos, pedido de audição perante a autoridade de controlo da proteção de dados e pedido de assistência executiva por parte da polícia).

[54] Artigo 47.º, n.º 2, alíneas a) a c), da Diretiva Proteção de Dados na Aplicação da Lei.

[55] Foram 18 os Estados-Membros que previram essa possibilidade: Bulgária, Chéquia, Estónia, Grécia, Croácia, Itália, Chipre, Letónia, Lituânia, Luxemburgo, Hungria, Malta, Países Baixos, Áustria, Portugal, Roménia, Eslováquia e Suécia. As autoridades de controlo da proteção de dados em três Estados-Membros (Estónia, Letónia e Áustria) podem aplicar coimas a pessoas singulares (por exemplo, trabalhadores) ou a entidades privadas (ou seja, entidades privadas que são subcontratantes de dados).

[56] Artigo 52.º da Diretiva Proteção de Dados na Aplicação da Lei.

apresentação de uma reclamação deste tipo. É importante que este prazo não prejudique o direito dos titulares dos dados a este respeito.

Em consonância com a Diretiva Proteção de Dados na Aplicação da Lei[57], todos os Estados-Membros preveem o direito de intentar ação judicial contra as decisões da autoridade de controlo, sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial disponível nos respetivos sistemas jurídicos. O direito de intentar ação judicial é admitido por todos os Estados-Membros, com exceção de dois[58], se uma autoridade de controlo não atender à reclamação nem informar o titular dos dados, no prazo de três meses, do andamento ou do resultado da reclamação[59].

A maioria dos Estados-Membros prevê igualmente o direito de intentar uma ação judicial contra o responsável pelo tratamento de dados e o subcontratante[60] em caso de alegada violação da Diretiva Proteção de Dados na Aplicação da Lei. Contudo, várias leis nacionais de transposição não preveem o direito de o titular dos dados mandatar organismos, organizações e associações sem fins lucrativos para apresentar reclamação junto de uma autoridade de controlo ou intentar uma ação judicial em seu nome[61].

2.2.4 Prazos para a conservação e avaliação

As abordagens dos Estados-Membros para transpor os prazos da Diretiva Proteção de Dados na Aplicação da Lei para a conservação dos dados pessoais e avaliação da necessidade de os conservar[62] variam consideravelmente. A maioria dos atos nacionais de proteção de dados que transpõem a Diretiva Proteção de Dados na Aplicação da Lei limita-se a cumprir o requisito geral do artigo 5.º da referida diretiva. Tal significa que cabe ao direito setorial fixar efetivamente os prazos para o apagamento de dados pessoais ou para uma avaliação periódica da necessidade de os conservar. Alguns Estados-Membros transpõem a disposição estabelecendo prazos na legislação setorial.

Contudo, em alguns Estados-Membros, a lei incumbe a autoridade competente de fixar os prazos. Em alguns casos, a lei não estabelece quaisquer critérios para a avaliação periódica, nem exige que esses critérios sejam previstos por outras leis e/ou não prevê que os procedimentos destinados a garantir o cumprimento dos prazos sejam igualmente estabelecidos no direito nacional.

Note-se que o Supremo Tribunal Administrativo da Bulgária solicitou recentemente ao TJUE que respondesse ao seu pedido de decisão prejudicial sobre a interpretação do artigo 5.º da Diretiva

[57] Artigo 53.º da Diretiva Proteção de Dados na Aplicação da Lei.
[58] Finlândia e Suécia.
[59] Artigo 53.º, n.º 2, da Diretiva Proteção de Dados na Aplicação da Lei.
[60] Artigo 54.º da Diretiva Proteção de Dados na Aplicação da Lei.
[61] Artigo 55.º da Diretiva Proteção de Dados na Aplicação da Lei.
[62] Artigo 5.º da Diretiva Proteção de Dados na Aplicação da Lei.

Proteção de Dados na Aplicação da Lei no que diz respeito aos prazos para o armazenamento de dados[63].

2.2.5 Base jurídica do tratamento, incluindo categorias especiais de dados pessoais

A maioria dos Estados-Membros prevê — utilizando muitas vezes uma formulação que se coaduna estreitamente com o artigo 8.º da Diretiva Proteção de Dados na Aplicação da Lei — que a base jurídica para o tratamento deve estar prevista no direito da UE ou dos Estados-Membros. Contudo, alguns atos nacionais de proteção de dados que transpõem a Diretiva Proteção de Dados na Aplicação da Lei não refletem o requisito de que os dados pessoais a tratar e as finalidades do tratamento devem estar especificados no direito[64]. Outros atos nacionais de proteção de dados que transpõem a Diretiva Proteção de Dados na Aplicação da Lei não contêm todas as disposições correspondentes ao artigo 8.º. Cabe à legislação nacional estabelecer a base do tratamento e cumprir os requisitos do artigo 8.º. Além disso, a mera repetição no direito nacional dos requisitos gerais do artigo 8.º da Diretiva Proteção de Dados na Aplicação da Lei não pode ser considerada uma base jurídica suficiente para uma operação de tratamento específica: o direito nacional deve especificar a autoridade competente para tratar os dados pessoais, as funções públicas que exerce e que justificam esse tratamento, bem como a finalidade do tratamento.

No que diz respeito ao tratamento de categorias especiais de dados pessoais[65], a maioria dos Estados-Membros exige como condição prévia para o tratamento a existência de necessidade estrita. A maioria dos Estados-Membros também prevê os mesmos fundamentos jurídicos para o tratamento de dados sensíveis que os previstos no artigo 10.º da Diretiva Proteção de Dados na Aplicação da Lei (tratamento autorizado pelo direito; destinado a proteger os interesses vitais do titular dos dados ou de outra pessoa singular; ou relacionado com dados manifestamente tornados públicos pelo seu titular). Em alguns Estados-Membros, a legislação de transposição prevê alguns motivos adicionais para o tratamento de dados (por exemplo, quando o tratamento desses dados é necessário para evitar ou prevenir um perigo que ameace diretamente a vida, a integridade física ou os bens das pessoas, ou para proteger a saúde ou os interesses da pessoa em causa ou de outra pessoa). Quando o ato nacional de proteção de dados que transpõe a Diretiva Proteção de Dados na Aplicação da Lei não prevê as garantias necessárias para os direitos e liberdades dos titulares dos dados (como é o caso em alguns Estados-Membros), tais garantias devem ser previstas na legislação setorial.

Algumas legislações nacionais de transposição referem o consentimento em relação ao tratamento de dados pessoais, incluindo o tratamento de categorias especiais de dados pessoais. É importante recordar que, embora os Estados-Membros não estejam impedidos de prever, na sua legislação nacional, que o titular dos dados possa concordar com o tratamento dos seus dados pessoais para os fins previstos na Diretiva Proteção de Dados na Aplicação da Lei, este consentimento só pode servir de salvaguarda e não pode constituir a base jurídica para esse tratamento. Os debates sobre

[63] Pedido de decisão prejudicial no processo NG/Direktor na Glavna direktsia «Natsionalna politsia» pri MVR — Sófia, C-118/22.
[64] Artigo 8.º, n.º 2, da Diretiva Proteção de Dados na Aplicação da Lei.
[65] Artigo 10.º da Diretiva Proteção de Dados na Aplicação da Lei.

esta questão indicam que seria útil dispor de mais orientações sobre o papel do consentimento no contexto do tratamento de dados pessoais para efeitos de aplicação do direito penal.

2.2.6 Decisões automatizadas

A legislação de transposição de todos os Estados-Membros inclui disposições que proíbem uma decisão tomada exclusivamente com base no tratamento automatizado, a menos que tal esteja previsto no direito[66]. A maior parte da legislação de transposição dos Estados-Membros exige que tais decisões não se baseiem em categorias especiais de dados pessoais, a menos que sejam dadas garantias adequadas[67]. Proíbem igualmente a definição de perfis que resulte em discriminação[68]. Contudo, em alguns casos, a legislação nacional não faz referência a garantias adequadas dos direitos e liberdades do titular dos dados quando as decisões automatizadas são autorizadas por lei. Mais especificamente, nem todos os Estados-Membros preveem o direito de obter a intervenção humana do responsável pelo tratamento nem exigem medidas adequadas para salvaguardar os direitos e/ou as liberdades e os interesses legítimos do titular dos dados.

2.2.7 Direitos dos titulares dos dados

Todos os Estados-Membros optaram por utilizar a possibilidade oferecida pela Diretiva Proteção de Dados na Aplicação da Lei de limitar o direito de acesso dos titulares dos dados aos seus dados pessoais[69]. A maioria dos Estados-Membros também prevê restrições a outros direitos dos titulares dos dados[70]. Frequentemente, os atos nacionais de proteção de dados que transpõem a diretiva limitam-se a seguir a linguagem geral da Diretiva Proteção de Dados na Aplicação da Lei sem especificar as circunstâncias ou as condições em que as restrições devem ser aplicadas. Nesses casos, estas circunstâncias e condições têm de ser especificadas na legislação setorial, sob pena de conceder aos responsáveis pelo tratamento de dados poderes discricionários na aplicação destas restrições.

A maioria dos Estados-Membros cumpre o requisito da Diretiva Proteção de Dados na Aplicação da Lei que permite aos titulares dos dados exercerem os seus direitos através da autoridade de controlo da proteção de dados[71]. Os Estados-Membros, na sua maioria, utilizaram a opção de estipular que os direitos dos titulares dos dados devem ser exercidos em conformidade com o direito nacional no contexto de investigações e processos penais nacionais[72].

A legislação de transposição de vários Estados-Membros não reflete todos os requisitos específicos da Diretiva Proteção de Dados na Aplicação da Lei no que diz respeito à forma como os direitos

---

[66] Artigo 11.º, n.º 1, da Diretiva Proteção de Dados na Aplicação da Lei.
[67] Artigo 11.º, n.º 2, da Diretiva Proteção de Dados na Aplicação da Lei.
[68] Artigo 11.º, n.º 3, da Diretiva Proteção de Dados na Aplicação da Lei.
[69] Artigo 15.º, n.º 1, da Diretiva Proteção de Dados na Aplicação da Lei.
[70] Artigo 13.º, n.º 3, e artigo 16.º, n.º 4.
[71] Artigo 17.º da Diretiva Proteção de Dados na Aplicação da Lei.
[72] Artigo 18.º da Diretiva Proteção de Dados na Aplicação da Lei.

dos titulares dos dados devem ser exercidos (por exemplo, formato e meios de comunicação das respostas, ausência de encargos).

Existe uma decisão prejudicial pendente[73] pedida por um órgão jurisdicional alemão sobre a interpretação das restrições ao direito de acesso dos titulares dos dados aos seus dados (artigo 15.º da Diretiva Proteção de Dados na Aplicação da Lei à luz do artigo 54.º da mesma diretiva), bem como sobre o direito a intentar ação judicial nos termos do artigo 47.º da Carta e sobre a liberdade de escolha de uma profissão nos termos do artigo 15.º da Carta.

2.2.8 Algumas disposições importantes específicas da Diretiva Proteção de Dados na Aplicação da Lei

Algumas disposições da Diretiva Proteção de Dados na Aplicação da Lei são específicas do contexto de aplicação do direito penal e não têm equivalente no RGPD.

Categorias dos titulares dos dados

A Diretiva Proteção de Dados na Aplicação da Lei obriga os Estados-Membros a exigirem que um responsável pelo tratamento faça uma distinção, se for caso disso e na medida do possível, entre os dados de diferentes categorias de titulares de dados, e a fornecerem exemplos dessas categorias [por exemplo, uma pessoa em relação à qual existam motivos fundados para crer que cometeu ou está prestes a cometer uma infração penal (um «suspeito»)][74]. A legislação de alguns Estados-Membros não especifica (em certa medida ou de todo) as categorias enumeradas na Diretiva Proteção de Dados na Aplicação da Lei. Ao especificar a categoria de «suspeitos», algumas legislações nacionais não exigem que existam «motivos fundados para crer que cometeram ou estão prestes a cometer uma infração penal». O acórdão que será proferido pelo TJUE no processo pendente Ministerstvo na vatreshnite raboti v B.C. clarificará ainda mais a interpretação da Diretiva Proteção de Dados na Aplicação da Lei no que diz respeito às categorias de titulares de dados, nomeadamente o requisito de que a classificação de um titular de dados como suspeito deve estar subordinada à existência de «motivos fundados para crer que cometeram ou estão prestes a cometer uma infração penal»[75].

Distinção entre classes de dados pessoais e verificação da sua qualidade

Os Estados-Membros preveem que os dados pessoais baseados em factos sejam, na medida do possível, distinguidos dos dados pessoais baseados em apreciações pessoais[76]. Também devem assegurar que não sejam transmitidos nem disponibilizados dados pessoais incorretos, incompletos ou desatualizados. Sempre que tenham sido transmitidos dados incorretos, os destinatários devem ser notificados sem demora e, nesses casos, os dados pessoais devem ser retificados, apagados ou o seu tratamento limitado. Embora a maioria dos Estados-Membros tenha transposto este requisito,

[73] Pedido de decisão prejudicial no processo TX/Bundesrepublik Deutschland, C-481/21.
[74] Artigo 6.º da Diretiva Proteção de Dados na Aplicação da Lei.
[75] Pedido de decisão prejudicial no processo Ministerstvo na vatreshnite raboti/B.C., C-205/21.
[76] Artigo 7.º da Diretiva Proteção de Dados na Aplicação da Lei.

algumas das medidas específicas exigidas não estão explicitamente previstas em várias legislações nacionais de transposição.

Registo cronológico

No total, 12 Estados-Membros[77] utilizaram a opção de adiar até maio de 2023 a adaptação do seu sistema de tratamento automatizado aos requisitos de registo cronológico[78].

A maioria dos Estados-Membros prevê a existência de registos cronológicos para as operações de tratamento nos sistemas de tratamento automatizado[79]. Algumas legislações nacionais não exigem o registo de todos os tipos de operações. A Diretiva Proteção de Dados na Aplicação da Lei estabelece os tipos mínimos de informações que os registos devem conter. Algumas legislações nacionais não incluíram todos os tipos de informação exigidos (por exemplo, a razão para a consulta ou divulgação de dados pessoais).

3 PRIMEIROS ENSINAMENTOS DA APLICAÇÃO E DO FUNCIONAMENTO DA DIRETIVA PROTEÇÃO DE DADOS NA APLICAÇÃO DA LEI

3.1 Reclamações e impacto positivo nos direitos dos titulares dos dados

A Diretiva Proteção de Dados na Aplicação da Lei assegura a proteção dos direitos e liberdades fundamentais das pessoas singulares e, em especial, do direito à proteção de dados. Proporciona um quadro abrangente para os direitos do titular dos dados e a forma como esses direitos podem ser exercidos, nomeadamente o seu direito à informação, ao acesso, à retificação ou ao apagamento dos seus dados pessoais, bem como à limitação do tratamento. A Diretiva Proteção de Dados na Aplicação da Lei aumentou a compreensão dos titulares dos dados sobre os seus direitos e a forma como podem exercê-los, o que se reflete num aumento do número de pedidos apresentados às autoridades competentes. A prática demonstrou que, entre os direitos conferidos aos titulares dos dados ao abrigo da Diretiva Proteção de Dados na Aplicação da Lei, os direitos de acesso e apagamento são os mais frequentemente invocados junto das autoridades competentes[80].

A Diretiva Proteção de Dados na Aplicação da Lei permite a imposição de limites a determinados direitos (o direito de acesso[81] e o direito de retificação ou apagamento[82]) e às informações que o responsável pelo tratamento deve fornecer ao titular dos dados em relação aos dados pessoais tratados[83]. Os titulares dos dados podem solicitar às autoridades de controlo da proteção de dados que revejam a limitação do direito em questão por parte de uma autoridade competente ou que

[77] A Alemanha utilizou esta opção para determinadas leis de transposição da Diretiva Proteção de Dados na Aplicação da Lei a nível federal e dos Länder.
[78] Artigo 63.º, n.º 2, da Diretiva Proteção de Dados na Aplicação da Lei.
[79] Artigo 25.º da Diretiva Proteção de Dados na Aplicação da Lei.
[80] Posição do Conselho e conclusões sobre a aplicação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 15.
[81] Artigo 15.º da Diretiva Proteção de Dados na Aplicação da Lei.
[82] Artigo 16.º da Diretiva Proteção de Dados na Aplicação da Lei.
[83] Artigo 13.º da Diretiva Proteção de Dados na Aplicação da Lei.

verifiquem se a limitação foi efetuada em conformidade com a Diretiva Proteção de Dados na Aplicação da Lei (exercício indireto do direito)[84]. Cerca de metade das autoridades de controlo da proteção de dados comunica ter recebido esse pedido[85]. A prática mostra que o número de pedidos recebidos pode variar significativamente (por exemplo, na Croácia, houve apenas um pedido deste tipo, mas na França foram recebidos mais de 1 500 pedidos)[86]. Embora as autoridades de controlo da proteção de dados tenham determinado, na sequência de uma verificação ou de uma revisão destas reclamações, que a maioria dos pedidos era inadmissível, em vários casos o responsável pelo tratamento dos dados foi intimado a retificar ou apagar os dados pessoais ou a limitar o tratamento dos dados pessoais, assegurando assim a correta aplicação das limitações[87].

A Diretiva Proteção de Dados na Aplicação da Lei prevê que um organismo, organização ou associação sem fins lucrativos apresente uma reclamação em nome de um titular de dados. Contudo, parece ser subutilizada (apenas quatro autoridades de controlo da proteção de dados comunicaram que tinham recebido essas reclamações de um organismo representativo[88]). Do mesmo modo, as organizações da sociedade civil comunicaram apenas um pequeno número de pedidos para apresentar uma reclamação deste tipo[89].

As pessoas também estão a utilizar cada vez mais o seu direito de apresentar reclamações às autoridades de controlo da proteção de dados, nomeadamente nos casos em que as autoridades competentes limitam o exercício dos direitos dos titulares dos dados. Mais de um terço das autoridades de controlo da proteção de dados comunicaram um aumento do número de reclamações recebidas na sequência da transposição da Diretiva Proteção de Dados na Aplicação da Lei nos seus Estados-Membros[90]. Algumas das reclamações mais frequentes recebidas pelas autoridades de controlo da proteção de dados diziam respeito à limitação do direito de acesso[91], ao direito de retificação ou apagamento[92] e ao direito à informação e respetivas limitações[93]. A seguir surgiam as reclamações relacionadas com o princípio da limitação da conservação, que exige que as autoridades competentes conservem os dados pessoais apenas durante o tempo necessário, e com o direito à informação.

---

[84] Artigo 17.º da Diretiva Proteção de Dados na Aplicação da Lei.
[85] Quatro autoridades de controlo da proteção de dados não recolhem estatísticas sobre os pedidos recebidos ao abrigo do artigo 17.º da Diretiva Proteção de Dados na Aplicação da Lei.
[86] Trata-se de pedidos apresentados desde a transposição da Diretiva Proteção de Dados na Aplicação da Lei até dezembro de 2021. Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei (respostas individuais das APD).
[87] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 50.
[88] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 33.
[89] Três organizações (no contexto das respostas aos questionários que lhes foram enviados pela Agência dos Direitos Fundamentais) comunicaram que tinham recebido um pedido e uma organização comunicou que tinha recebido mais do que um pedido.
[90] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 31.
[91] Artigo 15.º da Diretiva Proteção de Dados na Aplicação da Lei.
[92] Artigo 16.º da Diretiva Proteção de Dados na Aplicação da Lei.
[93] Artigo 13.º da Diretiva Proteção de Dados na Aplicação da Lei.

3.2 Maior sensibilização das autoridades competentes para a proteção de dados

Os Estados-Membros referem que a introdução da Diretiva Proteção de Dados na Aplicação da Lei tem tido e continua a ter um impacto significativo na sensibilização das autoridades competentes para a importância da proteção de dados[94]. Várias autoridades de controlo da proteção de dados manifestaram a sua opinião de que o maior impacto da Diretiva Proteção de Dados na Aplicação da Lei tem sido aumentar a sensibilização para as questões relacionadas com a proteção de dados e os direitos dos titulares dos dados, e a ênfase colocada nas mesmas[95]. Foi algo que também ficou demonstrado pelos intercâmbios entre as autoridades de controlo da proteção de dados e as autoridades competentes responsáveis pelos direitos dos titulares dos dados e as modalidades de exercício desses direitos[96]. Algumas autoridades competentes comunicaram que, por esse motivo, tinham afetado mais recursos à proteção de dados[97]. Tal incluiu o investimento na incorporação do princípio da privacidade desde a conceção e por defeito nos seus sistemas informáticos, o estabelecimento de períodos de conservação de dados, a aplicação do princípio da minimização dos dados e a comunicação de violações. Subsequentemente, comunicaram que a segurança global dos dados tratados melhorou[98].

As atividades de formação e sensibilização das autoridades de controlo da proteção de dados contribuem igualmente para a correta aplicação da Diretiva Proteção de Dados na Aplicação da Lei, e as autoridades de controlo são incumbidas de sensibilizar os responsáveis pelo tratamento de dados e os subcontratantes para as suas obrigações ao abrigo da referida diretiva[99].

Muitas autoridades de controlo da proteção de dados sensibilizam através da publicação de orientações. Alguns dos temas abrangidos pelas diferentes autoridades de controlo da proteção de dados incluem: prestar assistência ao poder judicial, ao Ministério Público e às autoridades policiais no cumprimento do princípio da responsabilização; proceder ao intercâmbio de dados pessoais com a polícia; nomear um encarregado da proteção de dados; realizar uma avaliação de impacto sobre a proteção de dados; tratar dados em domínios penais como a criminalidade organizada e o terrorismo; conservar registos das atividades de tratamento e registos cronológicos; realizar videovigilância; fornecer informações aos titulares dos dados; notificar violações de dados; obrigações dos responsáveis pelo tratamento; e o exercício dos direitos pelos particulares.

Contudo, oito autoridades de controlo da proteção de dados ainda não emitiram orientações e/ou instrumentos práticos para ajudar as autoridades competentes e os subcontratantes a cumprirem as suas obrigações.

---

[94] Posição do Conselho e conclusões sobre a aplicação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 21.
[95] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei (respostas individuais das APD).
[96] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 40, e posição do Conselho e conclusões sobre a aplicação da Diretiva Proteção de Dados na Aplicação da Lei, p. 9.
[97] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei n.º 70.
[98] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei n.º 70.
[99] Artigo 46.º, n.º 1, alínea d), da Diretiva Proteção de Dados na Aplicação da Lei.

Além disso, 12 autoridades de controlo da proteção de dados não promoveram qualquer ação de formação nem realizaram atividades de sensibilização destinadas às autoridades competentes ou aos subcontratantes nos termos da Diretiva Proteção de Dados na Aplicação da Lei[100]. Das autoridades de controlo da proteção de dados que realizaram essas atividades, os temas mais frequentes incluíram: tratamento de dados pela polícia, pelo Ministério Público, pelas autoridades judiciárias e pelas autoridades prisionais; definição dos respetivos domínios de aplicação do RGPD e da Diretiva Proteção de Dados na Aplicação da Lei; utilização de dados pessoais provenientes de redes sociais; tratamento de dados em ficheiros policiais; técnicas de videovigilância e megadados; tratamento de pedidos dos titulares dos dados; e o tratamento dos dados pessoais dos reclusos[101].

Outra inovação da Diretiva Proteção de Dados na Aplicação da Lei é a obrigação de os responsáveis pelo tratamento de dados designarem um encarregado para a proteção de dados (EPD), cujas funções incluem, entre outras tarefas, informar e aconselhar sobre os requisitos em matéria de proteção de dados, fiscalizar a conformidade com a Diretiva Proteção de Dados na Aplicação da Lei, prestar aconselhamento no que respeita às avaliações de impacto sobre a proteção de dados e controlar a sua realização[102]. Tal conduziu a uma maior sensibilização das autoridades competentes para as suas obrigações em matéria de proteção de dados, tendo igualmente um impacto positivo no cumprimento das regras de proteção de dados por parte das autoridades competentes, como também reconheceu o Conselho[103].

É importante investir no desenvolvimento e na maximização dos conhecimentos especializados dos EPD, a fim de ajudar as autoridades competentes a aplicarem a Diretiva Proteção de Dados na Aplicação da Lei de forma coerente[104]. Por conseguinte, a Comissão criou e viabiliza a rede para os responsáveis pela proteção de dados das autoridades competentes, das agências no domínio da justiça e dos assuntos internos e da Procuradoria Europeia. Esta rede é uma iniciativa permanente que se centra na aplicação da Diretiva Proteção de Dados na Aplicação da Lei pelas autoridades competentes dos Estados-Membros. O seu objetivo é proporcionar uma plataforma para a cooperação e o intercâmbio de conhecimentos especializados entre os EPD dos Estados-Membros. A Rede de Peritos em Proteção de Dados da Europol (EDEN) e as redes nacionais de EPD para as autoridades competentes são iniciativas importantes que ajudam os EPD das autoridades competentes a promover o intercâmbio de boas práticas e de informações sobre a aplicação da Diretiva Proteção de Dados na Aplicação da Lei.

3.3 Maior segurança dos dados, mas divergências nas notificações de violação de dados

[100] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei (respostas individuais das APD).
[101] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei n.os 41-42.
[102] Artigos 32.º a 34.º da Diretiva Proteção de Dados na Aplicação da Lei.
[103] Posição do Conselho e conclusões sobre a aplicação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 22.
[104] Posição do Conselho e conclusões sobre a aplicação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 25.

A Diretiva Proteção de Dados na Aplicação da Lei melhorou a segurança dos dados pessoais ao exigir que as autoridades competentes tomem medidas para alcançar objetivos de segurança específicos. Por exemplo, exige que as autoridades competentes realizem avaliações de impacto sobre a proteção de dados sempre que uma atividade de tratamento de dados seja suscetível de resultar num elevado risco para os direitos e as liberdades dos titulares dos dados. As avaliações de impacto implicam a identificação de riscos e de medidas para os atenuar. Este requisito, bem como a adesão obrigatória ao princípio da proteção de dados desde a conceção e por defeito e aos requisitos de notificação da violação de dados, permitiram melhorar a segurança do tratamento de dados pessoais[105].

O Conselho reconheceu igualmente este facto, tendo concluído que a Diretiva Proteção de Dados na Aplicação da Lei melhorou o nível de segurança dos dados, nomeadamente através de planos de segurança; da atualização dos sistemas informáticos e das medidas organizativas; de avaliações de impacto sobre a proteção de dados; e exigindo que as autoridades competentes mantenham registos relativos a operações de tratamento específicas[106].

A Diretiva Proteção de Dados na Aplicação da Lei estabelece as circunstâncias em que os responsáveis pelo tratamento de dados devem notificar a sua autoridade de controlo da proteção de dados e o titular dos dados em causa de uma violação de dados pessoais[107]. Não obstante esta obrigação, existe uma grande disparidade no número de violações de dados que foram notificadas às autoridades de controlo da proteção de dados desde a introdução da Diretiva Proteção de Dados na Aplicação da Lei[108]. Seis autoridades de controlo da proteção de dados comunicaram que não tinham recebido notificações de violação de dados[109] e várias outras comunicaram que tinham recebido muito poucas notificações desse tipo. Por exemplo, a autoridade italiana comunicou apenas três notificações de violação de dados e a autoridade francesa comunicou oito, mas a autoridade neerlandesa comunicou mais de 500.

Esta diferença no número de notificações de violações de dados comunicadas indica (após ter em conta fatores como a dimensão da população) que parecem existir práticas divergentes entre as autoridades competentes dos Estados-Membros no que diz respeito ao que é considerado uma violação e quando esta deve ser comunicada a uma autoridade de controlo da proteção de dados. A Comissão também referiu este facto no seu relatório sobre o RGPD[110]. O CEPD publicou

---

[105] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei, n.os 70 e 71, e respostas individuais da APD (Alemanha, Finlândia, França, Hungria e Malta).
[106] Posição do Conselho e conclusões sobre a aplicação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 26.
[107] Artigos 30.º e 31.º da Diretiva Proteção de Dados na Aplicação da Lei.
[108] Os valores incluem todas as violações de dados comunicadas entre a transposição da Diretiva Proteção de Dados na Aplicação da Lei e dezembro de 2021. Os dados foram recolhidos junto das autoridades de controlo da proteção de dados em dezembro de 2021.
[109] Espanha, Croácia, Lituânia, Portugal, Eslovénia e Eslováquia.
[110] Documento de trabalho dos serviços da Comissão, Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «A proteção de dados enquanto pilar da capacitação dos cidadãos e a abordagem da UE para a transição digital — dois anos de aplicação do Regulamento Geral sobre a Proteção de Dados», COM(2020) 264 final.

recentemente orientações sobre violações ao abrigo do RGPD[111]. Embora não sejam diretamente aplicáveis, essas orientações também são relevantes para as violações de dados no âmbito da Diretiva Proteção de Dados na Aplicação da Lei. Devem, por conseguinte, contribuir para uma abordagem mais uniforme do tratamento das violações de dados no âmbito da Diretiva Proteção de Dados na Aplicação da Lei em todos os Estados-Membros.

3.4 Supervisão pelas autoridades de controlo da proteção de dados

3.4.1 Recursos das autoridades de controlo da proteção de dados

Dotar cada autoridade de proteção de dados dos recursos humanos, técnicos e financeiros, das instalações e das infraestruturas necessários constitui um requisito prévio para o exercício eficaz das suas atribuições e dos seus poderes sendo, por conseguinte, uma condição essencial para a sua independência[112]. A Comissão tem repetidamente salientado que os Estados-Membros são obrigados a afetar recursos humanos, financeiros e técnicos suficientes às autoridades de controlo da proteção de dados[113]. O Conselho apelou também especificamente aos Estados-Membros para que atribuam recursos humanos, técnicos e financeiros suficientes às autoridades de controlo da proteção de dados[114].

Contudo, o aumento global do pessoal das autoridades de controlo da proteção de dados nos últimos anos[115] não parece dizer respeito às tarefas relacionadas com a Diretiva Proteção de Dados na Aplicação da Lei. A quantidade de pessoal que trabalha na Diretiva Proteção de Dados na Aplicação da Lei manteve-se inalterada ou chegou mesmo a diminuir em metade das autoridades de controlo da proteção de dados[116]. Qualquer aumento foi muito modesto, correspondendo, em média, a menos de duas pessoas em equivalentes a tempo completo («ETC»)[117]. Em quase metade das autoridades de controlo da proteção de dados (incluindo as que têm um número total de trabalhadores superior a 100 ETC), menos de 1 % a 7 % do total do pessoal trabalha na Diretiva

---

[111] Orientação 01/2021 do CEPD relativa a exemplos relacionados com a notificação de violações de dados pessoais, adotada em 14 de dezembro de 2021. https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf.

[112] Artigo 42.º, n.º 4, da Diretiva Proteção de Dados na Aplicação da Lei.

[113] Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «A proteção de dados enquanto pilar da capacitação dos cidadãos e a abordagem da UE para a transição digital — dois anos de aplicação do Regulamento Geral sobre a Proteção de Dados», COM(2020) 264 final.

[114] Posição do Conselho e conclusões sobre a aplicação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 12.

[115] Contributo do CEPD para a avaliação do RGPD nos termos do artigo 97.º, 18 de fevereiro de 2020, p. 26-29. https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf; Documento do CEPD intitulado *Overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities* (não traduzido para português) («documento do CEPD sobre uma panorâmica dos recursos»), 5 de agosto de 2021, p. 4-5. https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/overview-resources-made-available-member-states-data_en.

[116] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 65 e figura sobre o Q41, p. 20.

[117] A Alemanha indicou um aumento significativo de 33 para 53 ETC entre 2017 e 2021.

Proteção de Dados na Aplicação da Lei[118]. Em números absolutos, cerca de metade das autoridades de controlo da proteção de dados afeta entre 1 e 4 ETC a funções relacionadas com a Diretiva Proteção de Dados na Aplicação da Lei e oito autoridades de controlo da proteção de dados afetam entre 7 e 15 ETC a essas funções. Contudo, uma autoridade de controlo da proteção de dados dispõe de 53 ETC a trabalhar na Diretiva Proteção de Dados na Aplicação da Lei[119]. Do mesmo modo, o Secretariado do CEPD dedicou menos de 1,5 ETC a questões totalmente relacionadas com a Diretiva Proteção de Dados na Aplicação da Lei.

Esta situação não é satisfatória, ainda que dez autoridades de controlo da proteção de dados tenham indicado que dispõem de recursos financeiros, humanos e técnicos suficientes[120]. Por outro lado, 16 autoridades de controlo da proteção de dados consideraram que não dispõem de recursos suficientes. Destas autoridades, algumas observaram que esta situação afetou negativamente as investigações que realizaram por iniciativa própria[121], o seu tratamento das reclamações[122], a inspeção dos sistemas informáticos de grande escala (SIS, VIS) e a emissão de pareceres por sua própria iniciativa[123]. Com efeito, as características específicas do setor significam que a aplicação efetiva da Diretiva Proteção de Dados na Aplicação da Lei exige uma inspeção sistemática das atividades de tratamento, que são frequentemente complexas, e que as reclamações individuais não bastam (uma vez que são muito menos numerosas do que as do RGPD)[124].

Além disso, as autoridades de controlo da proteção de dados chamaram a atenção para a falta de conhecimentos informáticos especializados para fazer face à crescente complexidade das tecnologias informáticas utilizadas no domínio da aplicação da lei[125].

3.4.2 Utilização dos poderes

Utilização dos poderes de correção

No total, 19 autoridades de controlo da proteção de dados aplicaram os seus poderes de investigação, quer por iniciativa própria quer com base numa reclamação[126]. Foram muito poucos

[118] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei, figura sobre o Q41, p. 20. Documento do CEPD sobre uma panorâmica dos recursos, p. 5.
[119] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei figura sobre o Q41, p. 19.
[120] Bélgica, Dinamarca, Irlanda, Grécia, Letónia, Luxemburgo, Hungria, Malta, Áustria e Finlândia.
[121] Alemanha e França.
[122] França e Suécia.
[123] Países Baixos.
[124] A Irlanda recebeu 135 reclamações relacionadas com a Diretiva Proteção de Dados na Aplicação da Lei desde 2018, a Hungria recebeu 141 desde 2018 e a Dinamarca 223 desde 2017. Em contrapartida, houve milhares de reclamações relacionadas com o RGPD (ver o documento do CEPD sobre uma panorâmica dos recursos, p. 10).
[125] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 69.
[126] As autoridades de controlo da proteção de dados da Irlanda, de Malta e dos Países Baixos comunicaram que realizaram investigações por sua própria iniciativa. As autoridades de controlo da proteção de dados da Grécia, da Espanha, da Lituânia e da Hungria realizaram investigações com base em reclamações. As autoridades de controlo da proteção de dados da Bélgica, da Bulgária, da Dinamarca, da Alemanha, da França, da Itália, do Luxemburgo, da Áustria, da Polónia, da Eslovénia e da Suécia realizaram investigações tanto por sua própria iniciativa como com base em reclamações.

os casos em que as autoridades de controlo da proteção de dados comunicaram dificuldades (por exemplo, quando um responsável pelo tratamento não forneceu todas as informações pertinentes ou recusou o acesso à informação)[127].

As mesmas 19 autoridades de controlo da proteção de dados também aplicaram os seus poderes de correção. De longe, o poder mais frequentemente utilizado foi o de emitir ordens para tornar o tratamento conforme com a lei, nomeadamente ordens para retificar ou apagar dados pessoais ou para restringir o seu tratamento. As autoridades de controlo da proteção de dados utilizaram este poder em 114 casos. O facto de este poder de ordenar uma limitação temporária ou definitiva (incluindo uma proibição) do tratamento só ter sido utilizado em quatro casos[128] mostra que as autoridades de controlo da proteção de dados utilizaram cuidadosamente esses poderes.

Utilização dos poderes consultivos

A realização sistemática de consultas prévias e a solicitação do parecer das autoridades de controlo da proteção de dados sobre os projetos de medidas legislativas e administrativas constituem um meio eficaz para assegurar um elevado nível de proteção do direito à proteção dos dados pessoais e reduzir o número de reclamações subsequentes. A consulta prévia das autoridades de controlo da proteção de dados reveste-se de especial importância quando se trata da utilização de novas tecnologias que possam ter um impacto significativo nos direitos fundamentais.

Metade das autoridades de controlo da proteção de dados comunicou que tinham sido consultadas acerca das avaliações de impacto sobre a proteção de dados. O número de consultas prévias varia consoante os Estados-Membros. Algumas autoridades foram consultadas apenas uma vez, enquanto outra autoridade recebeu 59 consultas prévias[129]. Na maioria destes casos, as autoridades de controlo da proteção de dados prestaram aconselhamento escrito e, em alguns casos, utilizaram os seus poderes de correção em relação ao tratamento — em especial, emitiram advertências ou ordenaram a adoção de medidas que tornassem o tratamento de dados conforme com a lei. Num dos casos, a autoridade de controlo da proteção de dados emitiu um parecer negativo que parece ter tido o mesmo efeito que uma proibição de tratamento.

Além disso, afigura-se que as autoridades de controlo da proteção de dados também tratam pedidos de aconselhamento fora do procedimento de consulta prévia. O tipo de questão mais comum que levou as autoridades competentes a contactar as autoridades de controlo da proteção de dados para aconselhamento está relacionado com tipos específicos de tratamento (em especial, a utilização de

[127] As autoridades de controlo da proteção de dados alemãs e húngaras declararam que não tinham recebido todas as informações necessárias e/ou que o responsável pelo tratamento lhes recusou o acesso às informações necessárias. As autoridades alemãs referiram que não está previsto um poder semelhante ao do artigo 58.º, n.º 1, alínea a), do RGPD.
[128] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 30, bem como as respostas individuais das autoridades da Áustria e do Luxemburgo.
[129] As autoridades de controlo da proteção de dados dinamarquesas e lituanas comunicaram que tinham sido consultadas apenas uma vez. A autoridade de controlo da proteção de dados belga recebeu 59 consultas prévias.

novas tecnologias, mecanismos ou procedimentos; logo em seguida, medidas de segurança adequadas, o tratamento de categorias especiais de dados pessoais, a determinação da base jurídica para o tratamento, o princípio da limitação da conservação e prazos adequados[130]).

Além disso, 22 autoridades de controlo da proteção de dados emitiram pareceres aos respetivos parlamentos e governos nacionais sobre medidas legislativas e administrativas relacionadas com o tratamento de dados pessoais. Várias indicaram que são consultadas ocasionalmente[131].

3.4.3 Controlo jurisdicional das ações das autoridades de controlo da proteção de dados

Quase metade das autoridades de controlo da proteção de dados referiu que, num número reduzido de casos, tiveram de fazer face a processos judiciais relacionados com as suas decisões ou inações. Os processos foram instaurados principalmente pelos titulares dos dados e, em alguns casos, pelas autoridades competentes[132]. Vários processos tinham sido declarados inadmissíveis pelos tribunais ou tinham sido retirados pelos autores. O tribunal confirmou a decisão da autoridade de controlo da proteção de dados na maior parte dos restantes processos, mas anulou-a noutros processos (e outros processos ainda estavam pendentes). O reduzido número de sentenças proferidas até à data significa que ainda não é possível detetar uma tendência clara.

3.4.4 Orientações do CEPD

A coerência e um elevado nível de proteção entre os Estados-Membros são fundamentais para assegurar a eficácia da cooperação judiciária em matéria penal e da cooperação policial[133]. A Diretiva Proteção de Dados na Aplicação da Lei prevê que o CEPD emita orientações, recomendações e boas práticas (por sua própria iniciativa ou a pedido da Comissão), a fim de assegurar que os Estados-Membros aplicam a referida diretiva de forma coerente. O CEPD elaborou orientações específicas para a Diretiva Proteção de Dados na Aplicação da Lei pertinentes para o capítulo V (transferências internacionais)[134]; orientações sobre a utilização de tecnologias de reconhecimento facial[135]; e (na sua antiga qualidade de Grupo de Trabalho do artigo 29.º) um

---

[130] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 39.
[131] As autoridades de controlo da proteção de dados da Chéquia, da Grécia, da Croácia, da Letónia e da Suécia comunicaram que não emitiram pareceres. As autoridades de controlo da proteção de dados da Grécia, da Croácia, da Letónia, da Polónia, da Roménia, da Eslovénia e da Eslováquia só foram consultadas ocasionalmente.
[132] Esta observação baseia-se nas respostas recebidas das autoridades de controlo da proteção de dados da Bélgica, da Bulgária, da Alemanha, da Estónia, da Irlanda, da Itália, da Hungria, dos Países Baixos, da Áustria, da Polónia, da Finlândia e da Suécia.
[133] Considerando 7 da Diretiva Proteção de Dados na Aplicação da Lei.
[134] Recomendações do CEPD intituladas «Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive» (não traduzidas para português), adotadas em 2 de fevereiro de 2021. https://edpb.europa.eu/sites/default/files/files/file1/recommendations012021onart.36led.pdf_en.pdf.
[135] Orientações do CEPD intituladas «Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement» (não traduzidas para português), adotadas em 12 de maio de 2022, versão para consulta pública disponível em https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.

parecer sobre algumas questões fundamentais da Diretiva Proteção de Dados na Aplicação da Lei[136].

Muitas das orientações do CEPD sobre o RGPD são igualmente relevantes para a Diretiva Proteção de Dados na Aplicação da Lei, na medida em que se baseiam em conceitos ou tecnologias comuns. Essas orientações incluem as relacionadas com o conceito de responsável pelo tratamento de dados e subcontratante[137], os direitos dos titulares dos dados[138], a notificação de violações dos dados pessoais[139], a avaliação de impacto sobre a proteção de dados[140], a proteção de dados desde a conceção e por defeito[141] e as decisões individuais automatizadas[142].

A elaboração de orientações abrangentes e práticas exige uma quantidade significativa de trabalho e de recursos, mas as orientações são essenciais (como também observou o Conselho[143]). Por conseguinte, é muito positivo que o CEPD tenha indicado que, em breve, fornecerá orientações adicionais, nomeadamente sobre o conceito de poderes de investigação e de correção eficazes das autoridades de controlo da proteção de dados e sobre as transferências internacionais que estão sujeitas a garantias adequadas.

---

[136] Parecer do Grupo de Trabalho do artigo 29.º intitulado «Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)», WP 258, adotado em 29 de novembro de 2017, disponível em https://ec.europa.eu/newsroom/article29/items/610178/en.

[137] Orientações do CEPD intituladas «Guidelines 07/2020 on the concepts of data controller and processor in the GDPR» (não traduzidas para português), adotadas em 7 de julho de 2021, disponíveis em: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf.

[138] Orientações do CEPD intituladas «Guidelines 01/2022 on data subject rights — Right of access» (não traduzidas para português), adotadas em 18 de janeiro de 2022, versão para consulta pública disponível em https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.

[139] Orientações do Grupo de Trabalho do artigo 29.º intituladas «Guidelines on Personal data breach notification under Regulation 2016/679» (não traduzidas para português), WP 250rev.01, revistas pela última vez em 6 de fevereiro de 2018 e aprovadas pelo CEPD em 25 de maio de 2018, disponíveis em https://ec.europa.eu/newsroom/article29/items/612052/en; orientações do CEPD intituladas «Guidelines 01/2021 on examples regarding personal data breach notification» (não traduzidas para português), adotadas em 14 de dezembro de 2021, disponíveis em: https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf.

[140] Orientações do Grupo de Trabalho do artigo 29.º intituladas «Guidelines on Data Protection Impact Assessment (DPIA) and determining whether
processing is "likely to result in a high risk" for the purposes of Regulation 2016/679» (não traduzidas para português), WP 248rev.01, revistas pela última vez em 4 de outubro de 2017 e aprovadas pelo CEPD em 25 de maio de 2018, disponíveis em: https://ec.europa.eu/newsroom/article29/items/611236.

[141] Orientações do CEPD intituladas «Guidelines 4/2019 on Article 25 data protection by design and by default» (não traduzidas para português), adotadas em 20 de outubro de 2020, disponíveis em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[142] Orientações do Grupo de Trabalho do artigo 29.º intituladas «Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679» (não traduzidas para português), WP 251rev01, revistas pela última vez em 6 de fevereiro de 2018 e aprovadas pelo CEPD em 25 de maio de 2018; disponíveis em: https://ec.europa.eu/newsroom/article29/items/612053/en.

[143] Posição do Conselho e conclusões sobre a aplicação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 14.

As orientações do CEPD podem também reduzir o volume de trabalho das autoridades de controlo da proteção de dados (por exemplo, tarefas como aconselhamento aos responsáveis pelo tratamento de dados ou tratamento de reclamações). Por exemplo, várias das questões abordadas no parecer do Grupo de Trabalho do artigo 29.º sobre alguns elementos fundamentais da Diretiva Proteção de Dados na Aplicação da Lei (nomeadamente, prazos adequados, base jurídica do tratamento, condições para o tratamento de categorias especiais de dados) são também algumas das questões mais frequentes sobre as quais as autoridades competentes solicitaram aconselhamento às autoridades de controlo da proteção de dados[144].

3.4.5 Assistência mútua

A fim de assegurar a aplicação coerente da Diretiva Proteção de Dados na Aplicação da Lei, as autoridades de controlo da proteção de dados são obrigadas a prestar assistência mútua entre si. Tal inclui a assistência sob a forma de pedidos de informação e pedidos de realização de consultas, inspeções e inquéritos[145]. Contudo, até à data, a assistência mútua tem sido muito raramente utilizada. Apenas seis autoridades de controlo da proteção de dados a utilizaram, principalmente em resposta a pedidos de informação recebidos de outras autoridades de controlo da proteção de dados. A maioria das autoridades de controlo da proteção de dados indicou ter recebido apenas um pedido de informações. Todas estas autoridades de controlo da proteção de dados comunicaram que cumpriram o pedido recebido. O intercâmbio voluntário de assistência mútua, que não tem um prazo legal nem uma obrigação estrita de resposta, também não foi utilizado. O CEPD declarou que publicará orientações sobre o quadro de assistência mútua ao abrigo do RGPD e da Diretiva Proteção de Dados na Aplicação da Lei[146].

3.5 Instrumento flexível para as transferências internacionais de dados

O capítulo V da Diretiva Proteção de Dados na Aplicação da Lei abrange as transferências de dados pessoais para as autoridades competentes de países terceiros e organizações internacionais. Este capítulo visa essencialmente assegurar a continuidade da proteção quando os dados pessoais são transferidos de um Estado-Membro para um país terceiro ou uma organização internacional para efeitos de aplicação da lei. Tal como acima referido, essa continuidade da proteção é uma condição importante para uma cooperação policial rápida, eficaz e juridicamente segura entre parceiros de confiança.

Em especial, nos termos das regras pertinentes da Diretiva Proteção de Dados na Aplicação da Lei[147], as transferências internacionais entre autoridades competentes na aceção da Diretiva Proteção de Dados na Aplicação da Lei devem basear-se num dos vários instrumentos de transferência previstos nos artigos 36.º a 38.º da Diretiva Proteção de Dados na Aplicação da Lei

---

[144] Contributo do CEPD para a avaliação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 39.
[145] Artigo 50.º da Diretiva Proteção de Dados na Aplicação da Lei.
[146] Programa de trabalho 2021/2022 do CEPD, edpb_workprogramme_2021-2022_en.pdf (europa.eu).
[147] Ver o artigo 35.º, n.º 3, e o considerando 64 da Diretiva Proteção de Dados na Aplicação da Lei. No que diz respeito às transferências ulteriores, ver o artigo 35.º, n.º 1, alínea e), e o considerando 65 da Diretiva Proteção de Dados na Aplicação da Lei.

(se os dados forem provenientes de outro Estado-Membro, a transferência também exige a autorização prévia desse Estado-Membro). Estes instrumentos incluem decisões de adequação, transferências baseadas em salvaguardas adequadas e a utilização de derrogações em situações específicas. O artigo 39.º da Diretiva Proteção de Dados na Aplicação da Lei permite igualmente transferências diretas para destinatários que não sejam autoridades de aplicação do direito penal, estabelecidas em países terceiros, em casos individuais e específicos, e sujeitas a várias condições.

3.5.1 Decisões de adequação

A Comissão acelerou os seus trabalhos para realizar todo o potencial dos instrumentos disponíveis nos termos da Diretiva Proteção de Dados na Aplicação da Lei. Tal incluiu a adoção, pela primeira vez, de uma «decisão de adequação» que abrange as atividades de tratamento de dados para fins de aplicação da lei segundo o disposto no artigo 36.º da Diretiva Proteção de Dados na Aplicação da Lei, com o Reino Unido, em junho de 2021[148]. Esta decisão de adequação permite a circulação segura e livre de dados pessoais para as autoridades competentes do país terceiro em causa, sem necessidade de quaisquer outras garantias ou de uma autorização específica (a menos que outro Estado-Membro junto do qual os dados foram obtidos tenha de autorizar a transferência[149]). A decisão de adequação aplicável ao Reino Unido desde junho de 2021 é uma base fundamental para a cooperação policial e judiciária após o Brexit, que, segundo o Acordo de Comércio e Cooperação UE-Reino Unido, se baseia «no compromisso de longa data assumido pelas Partes de assegurar um elevado nível de proteção dos dados pessoais»[150]. Nos termos do artigo 36.º, n.º 4, da Diretiva Proteção de Dados na Aplicação da Lei, a Comissão controla quaisquer desenvolvimentos do quadro jurídico do Reino Unido que possam afetar esta decisão de adequação. Esta decisão de adequação com o Reino Unido é aplicável por um período de quatro anos a contar da sua entrada em vigor, prorrogável, em princípio, por mais quatro anos, se o controlo da Comissão confirmar que o Reino Unido continua a manter um nível de proteção adequado[151].

Além disso, o CEPD também contribuiu para o desenvolvimento deste instrumento, clarificando a norma jurídica através de orientações sobre os elementos que devem ser tidos em conta na avaliação da adequação no contexto da aplicação da lei, com a emissão do seu referencial de

---

[148] Decisão de Execução da Comissão nos termos da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais assegurado pelo Reino Unido, de 28 de junho de 2021, disponível em https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_en.pdf.

[149] Ver o artigo 35.º, n.º 1, alínea c), o artigo 35.º, n.º 2, e o considerando 66 da Diretiva Proteção de Dados na Aplicação da Lei.

[150] Ver o artigo 525.º, n.º 1, do ACC.

[151] Ver os n.ºs 172 a 174 da decisão intitulada «Decision on the adequate protection of personal data by the United Kingdom: Law Enforcement Directive» (não traduzida para português), 28 de junho de 2021, disponível em https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-united-kingdom-law-enforcement-directive_en.

adequação ao abrigo da Diretiva Proteção de Dados na Aplicação da Lei[152]. Em especial, o país terceiro deve assegurar direitos individuais oponíveis, vias de recurso judicial efetivas e uma supervisão independente.

A Comissão está a promover ativamente a possibilidade de emitir decisões de adequação com outros parceiros internacionais importantes, em especial aqueles com os quais é necessária uma cooperação estreita e rápida na luta contra a criminalidade e o terrorismo, e com os quais já são realizados importantes intercâmbios de dados pessoais[153]. Embora, até à data, não tenham sido adotadas outras decisões de adequação, tal deve-se sobretudo ao facto de este instrumento só ter sido introduzido recentemente. Além disso, e ao contrário do que acontece com o tratamento de dados por operadores comerciais, a convergência global das regras de proteção de dados no domínio da aplicação do direito penal está agora a começar a desenvolver-se (impulsionada, por exemplo, por acordos multilaterais, como a Convenção 108 modernizada do Conselho da Europa ou o Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime). Não obstante, a experiência adquirida com a adoção da decisão de adequação com o Reino Unido contribuirá para preparar o terreno para iniciativas semelhantes nos próximos anos. No âmbito da sua estratégia internacional, a Comissão considerará outros possíveis candidatos a futuras decisões de adequação ao abrigo da Diretiva Proteção de Dados na Aplicação da Lei, em contacto direto com as outras instituições e organismos pertinentes da UE[154]. Para o efeito, e em conformidade com o considerando 68 da Diretiva Proteção de Dados na Aplicação da Lei, a Comissão prestará especial atenção aos compromissos internacionais dos países avaliados em matéria de proteção de dados pessoais, nomeadamente a adesão aos referidos acordos multilaterais ou a outros instrumentos de aplicação da lei que prevejam garantias adequadas em matéria de proteção de dados.

3.5.2 Garantias adequadas

A Diretiva Proteção de Dados na Aplicação da Lei contém outros instrumentos de transferência para além da solução global de uma decisão de adequação. A flexibilidade deste «conjunto de ferramentas» está refletida no artigo 37.º da Diretiva Proteção de Dados na Aplicação da Lei, que regula as transferências de dados com base em «garantias adequadas» em matéria de proteção de dados pessoais. Essas garantias adequadas podem ser prestadas através de um instrumento juridicamente vinculativo ou quando o responsável pelo tratamento, com base numa avaliação de todas as circunstâncias que rodeiam a transferência, concluir que existem garantias adequadas (a chamada «autoavaliação» para as transferências).

---

[152] Recomendações do CEPD intituladas «Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive» (não traduzidas para português), adotadas em 2 de fevereiro de 2021. Ver também o artigo 36.º, n.º 2, e o considerando 67 da Diretiva Proteção de Dados na Aplicação da Lei.

[153] Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Intercâmbio e proteção de dados pessoais num mundo globalizado», COM(2017) 7 final, p. 13-14.

[154] Posição do Conselho e conclusões sobre a aplicação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 18.

Nos primeiros anos de aplicação da Diretiva Proteção de Dados na Aplicação da Lei, a Comissão trabalhou, em especial, nos instrumentos jurídicos vinculativos sob a forma de acordos internacionais que preveem salvaguardas adequadas. Estes acordos desempenham um papel importante tanto no contexto da cooperação «tradicional» (ou seja, da cooperação entre as autoridades competentes) como de outras formas de cooperação policial (ou seja, cooperação que envolva terceiros, como por exemplo empresas privadas). Podem também servir de base para as transferências de dados efetuadas pela Europol e pela Eurojust ao abrigo dos respetivos quadros jurídicos, cujas regras em matéria de transferências internacionais são muito semelhantes às previstas na Diretiva Proteção de Dados na Aplicação da Lei.

No que diz respeito às formas tradicionais de cooperação policial, a Comissão está a rever os acordos internacionais adotados antes da entrada em vigor da Diretiva Proteção de Dados na Aplicação da Lei, a fim de assegurar a coerência com o regime modernizado de proteção de dados da UE[155].

Em primeiro lugar, a Comissão está a avaliar as disposições em matéria de proteção de dados contidas nos acordos de cooperação da Europol[156] com países terceiros celebrados antes de 1 de maio de 2017, nos termos do Regulamento (UE) 2016/794 que cria a Agência da União Europeia para a Cooperação Policial (a seguir designado por «Regulamento Europol»)[157]. Em consonância com o artigo 9.º do Protocolo n.º 36 do Tratado da União Europeia[158] e com o TFUE (relativo às disposições transitórias), os efeitos jurídicos destes acordos foram preservados até que esses acordos sejam revogados, anulados ou alterados[159]. A Comissão informará o Parlamento Europeu e o Conselho do resultado desta avaliação e, se necessário, apresentará ao Conselho uma recomendação de decisão que autorize a abertura de negociações para alterar o(s) respetivo(s) acordo(s) em conformidade com o artigo 218.º do TFUE. Trata-se de uma tarefa complexa, que envolve a avaliação de 18 acordos e que sofreu atrasos devido às perturbações causadas pela pandemia de COVID-19. A Comissão espera concluir a sua avaliação no segundo semestre de 2022.

---

[155] Na sua Comunicação intitulada «Ações futuras para alinhar o acervo do antigo terceiro pilar com as regras de proteção de dados», a Comissão concluiu que vários acordos existentes não necessitam de um maior alinhamento com a Diretiva Proteção de Dados na Aplicação da Lei (por exemplo, o Acordo entre a União Europeia e a República da Islândia e o Reino da Noruega sobre a aplicação de determinadas disposições da Convenção de 29 de maio de 2000 relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia e do protocolo de 2001 a esta convenção).

[156] Para mais informações sobre os acordos da Europol em vigor, consultar o sítio Web da Europol em: https://www.europol.europa.eu/partners-collaboration/agreements.

[157] Ver o artigo 25.º, n.º 4, do Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho (JO L 135 de 24.5.2016, p. 53).

[158] Versão consolidada do Tratado sobre a União Europeia (JO C 202 de 7.6.2016, p. 13), disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A02016M%2FTXT-20200301.

[159] Considerando 35 do Regulamento Europol.

A coerência de todos os mecanismos de cooperação policial com as regras da Diretiva Proteção de Dados na Aplicação da Lei é um princípio orientador que a Comissão também segue aquando da negociação de novos acordos para a transferência de dados pessoais pela Europol para países terceiros ou organizações internacionais. Desde a entrada em vigor do atual Regulamento Europol, em 2017, que o artigo 218.º do TFUE constitui a base jurídica para esses acordos internacionais, assegurando a existência de garantias adequadas. Em 2018 e 2019, o Conselho adotou nove mandatos para que a Comissão iniciasse negociações com países terceiros em nome da União. A Comissão foi igualmente autorizada a encetar negociações sobre um acordo de cooperação com a Interpol para abranger o intercâmbio de dados com vários órgãos e organismos da UE. Em todos estes casos, o Conselho forneceu diretrizes de negociação à Comissão com vista a assegurar a inclusão das garantias necessárias para a proteção dos dados pessoais e de outros direitos e liberdades fundamentais das pessoas. Nesta base, a Comissão já concluiu as negociações com a Nova Zelândia, que conduziram à assinatura de um acordo de cooperação em 30 de junho de 2022. Além disso, registaram-se progressos nas negociações com Israel. No que diz respeito à Turquia, as negociações encontram-se numa fase avançada, mas não podem ser concluídas enquanto a Turquia não adotar as reformas necessárias na sua legislação em matéria de proteção de dados. Em março de 2021, foram concedidas autorizações semelhantes para a negociação de acordos de cooperação, a fim de permitir o intercâmbio de dados pela Eurojust com 13 países terceiros.

Em segundo lugar, a Comissão procede à primeira revisão conjunta do Acordo entre os Estados Unidos da América e a União Europeia sobre a proteção dos dados pessoais no âmbito da prevenção, investigação, deteção e repressão de infrações penais (Acordo-Quadro). O Acordo-Quadro, que entrou em vigor em fevereiro de 2017, contém um conjunto abrangente e harmonizado de regras de proteção de dados aplicáveis a todos os intercâmbios transatlânticos entre autoridades competentes. Complementa os acordos existentes entre a UE e os EUA e entre os Estados-Membros da UE e os EUA entre as autoridades responsáveis pela aplicação da lei, estabelece um nível elevado de proteção para futuros acordos neste domínio e reforça a cooperação em matéria de aplicação da lei, facilitando o intercâmbio de informações. A revisão conjunta pretende avaliar a eficácia da aplicação do Acordo-Quadro, em especial no que diz respeito às disposições relativas à transferência ulterior, aos direitos individuais e às vias de recurso judicial. O calendário para a revisão conjunta foi afetado pelas perturbações relacionadas com a pandemia de COVID-19, bem como pelas negociações paralelas sobre o Segundo Protocolo Adicional à Convenção de Budapeste do Conselho da Europa sobre o Cibercrime[160]. A Comissão prevê a sua conclusão no segundo semestre de 2022.

[160] A Comissão, em nome da União Europeia, e os Estados Unidos estiveram extremamente empenhados nestas negociações, nomeadamente no subgrupo dedicado à proteção de dados (sendo a proteção de dados um dos temas objeto de intenso debate).

Sendo o primeiro acordo internacional bilateral com um conjunto abrangente de direitos e obrigações em matéria de proteção de dados, o Acordo-Quadro constitui um ponto de referência para a negociação de acordos-quadro semelhantes com importantes parceiros responsáveis pela aplicação do direito penal[161]. Quando fizer essa negociação, a Comissão também terá em conta os desenvolvimentos pertinentes, nomeadamente as orientações do CEPD, a jurisprudência do TJUE e o resultado das negociações internacionais sobre as salvaguardas em matéria de proteção de dados neste domínio (como, por exemplo, o Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime ou o acordo da Europol com a Nova Zelândia[162]).

Em terceiro lugar, a Comissão identificou o Acordo entre a União Europeia e o Japão no domínio do auxílio judiciário mútuo em matéria penal (MLAT UE-Japão)[163] como um ato da UE que regula o tratamento de dados (transferências) para efeitos de aplicação do direito penal, o qual deve ser alterado para assegurar a existência de garantias adequadas em matéria de proteção de dados, em conformidade com a Diretiva Proteção de Dados na Aplicação da Lei. Na sequência da adoção pelo Conselho de uma decisão[164] que autoriza a abertura de negociações para alterar o MLAT UE-Japão, a Comissão continua a dialogar com as autoridades japonesas com vista a começar as negociações o mais rapidamente possível.

Além disso, são cada vez mais utilizadas outras formas de cooperação adaptadas aos desafios e necessidades específicos das investigações penais na economia digital atual. Estas formas de cooperação dizem respeito, sobretudo, ao reforço da cooperação no domínio da cibercriminalidade e à recolha de provas em formato eletrónico relativas a infrações penais. Esta cooperação, nomeadamente a cooperação direta com entidades privadas para o acesso a provas eletrónicas.

A Comissão também colaborou com parceiros internacionais com vista a assegurar que estas outras formas de cooperação (importantes) possam ocorrer com base em garantias adequadas em matéria de proteção de dados.

Em primeiro lugar, a Comissão representou a UE durante as negociações[165] no âmbito do Conselho da Europa sobre um Segundo Protocolo Adicional à Convenção de Budapeste sobre a

---

[161] Ver a Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Intercâmbio e proteção de dados pessoais num mundo globalizado», COM(2017) 7 final, p. 14.
[162] Acordo entre a União Europeia, por um lado, e a Nova Zelândia, por outro, sobre o intercâmbio de dados pessoais entre a Agência da União Europeia para a Cooperação Policial (Europol) e as autoridades neozelandesas competentes em matéria de luta contra a criminalidade grave e o terrorismo.
[163] Acordo entre a União Europeia e o Japão no domínio do auxílio judiciário mútuo em matéria penal (JO L 39 de 12.2.2010, p. 20).https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A22010A0212%2801%29
[164] Decisão do Conselho que autoriza a abertura de negociações com o Japão tendo em vista a alteração do Acordo entre a União Europeia e o Japão no domínio do auxílio judiciário mútuo em matéria penal (documento LT 223/21).
[165] Na sequência da aprovação de um mandato pelo Conselho da União Europeia em 6 de junho de 2019. O mandato está disponível em https://www.consilium.europa.eu/pt/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/.

Cibercriminalidade[166]. O Protocolo, aprovado pelo Comité de Ministros do Conselho da Europa em 17 de novembro de 2021, contém fortes salvaguardas para a proteção dos direitos fundamentais, nomeadamente um artigo[167] que contém disposições pormenorizadas sobre a proteção dos dados pessoais transferidos ao abrigo do Protocolo. Estas disposições abrangem todos os princípios, direitos e obrigações essenciais em matéria de proteção de dados reconhecidos no direito da UE. Estas garantias são complementadas por uma disposição de controlo e pela possibilidade de suspender as transferências em caso de violação sistemática ou material das salvaguardas previstas no Protocolo, por exemplo, a ausência de vias de recurso judicial eficazes. Através destas disposições, prevê garantias adequadas, em conformidade com os requisitos do artigo 37.º, n.º 1, alínea a), da Diretiva Proteção de Dados na Aplicação da Lei[168]. Trata-se de uma conquista significativa, dada a diversidade de membros da Convenção de Budapeste, que conta atualmente com 66 Estados Partes, os quais representam contextos jurídicos e tradições diferentes. Permitirá às autoridades competentes dos Estados-Membros beneficiar de uma cooperação transfronteiriça eficaz na luta contra a cibercriminalidade, assegurando simultaneamente o respeito pelos valores da UE refletidos na Carta dos Direitos Fundamentais da UE, nos Tratados da UE e no direito derivado da UE. Tendo em conta o grande número de Partes na Convenção de Budapeste, que inclui atualmente países de todo o mundo, o Protocolo contribuirá igualmente para promover normas exigentes de proteção de dados para o tratamento de dados no domínio da aplicação do direito penal a nível mundial. O Protocolo foi aberto à assinatura em 12 de maio de 2022, tendo já sido assinado por um total de 22 Partes na Convenção de Budapeste (incluindo 13 Estados-Membros da UE).

Em segundo lugar, a Comissão iniciou negociações com vista a um acordo bilateral com os Estados Unidos sobre o acesso transfronteiras a provas eletrónicas para fins de cooperação judiciária em matéria penal[169]. Este acordo visa abranger as provas eletrónicas sob a forma de dados pessoais e não pessoais, nomeadamente dados de tráfego e de conteúdo. Mais importante ainda, as negociações visam também a inclusão de salvaguardas adicionais em matéria de proteção de dados que complementem as previstas no Acordo-Quadro, tendo em conta, em especial, a natureza sensível das categorias de dados em causa, bem como os requisitos da transferência de provas

[166] O Segundo Protocolo Adicional à Convenção sobre o Cibercrime relativo ao reforço da cooperação e da divulgação de provas eletrónicas foi aprovado pelo Comité de Ministros do Conselho da Europa em 17 de novembro de 2021. Foi elaborado pelo Comité da Convenção sobre a Cibercriminalidade (T-CY) entre setembro de 2017 e maio de 2021. O texto do Protocolo (cópia autenticada) está disponível em: https://rm.coe.int/1680a4b2e1. O relatório explicativo do Protocolo está igualmente disponível em: https://rm.coe.int/1680a49c9d.

[167] Ver o artigo 14.º do Protocolo Adicional, juntamente com os n.os 220 a 287 do relatório explicativo.

[168] No seu Parecer 1/2022, de 20 de janeiro de 2022, sobre os projetos de decisões do Conselho que autorizam a assinatura e a ratificação do Protocolo Adicional, a AEPD «regista com agrado as várias salvaguardas que foram incluídas no Protocolo».

[169] Decisão do Conselho que autoriza a abertura de negociações tendo em vista a celebração de um acordo entre a União Europeia e os Estados Unidos da América sobre o acesso transfronteiras a provas eletrónicas para fins de cooperação judiciária em matéria penal. O mandato está disponível no seguinte endereço: https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/pt/pdf.

eletrónicas diretamente pelos prestadores de serviços. O progresso destas negociações dependerá, em grande medida, dos progressos do processo legislativo em curso sobre o pacote de provas eletrónicas da UE[170].

Estas várias iniciativas da Comissão para desenvolver instrumentos internacionais que facilitem a cooperação policial com parceiros internacionais, assegurando simultaneamente garantias adequadas em matéria de proteção de dados, foram apoiadas pelo trabalho do CEPD e da AEPD. Este trabalho inclui a declaração do CEPD sobre o projeto de Segundo Protocolo Adicional à Convenção de Budapeste[171] e os pareceres da AEPD sobre os projetos de mandatos de negociação de acordos internacionais nos termos do artigo 218.º do TFUE que permitiriam à Europol e à Eurojust proceder ao intercâmbio de dados pessoais com países terceiros ou organizações internacionais[172]. O CEPD emitiu igualmente uma declaração em que insta os Estados-Membros a avaliar e, se necessário, a rever os acordos internacionais que envolvem transferências internacionais de dados pessoais[173]. Essa declaração diz respeito aos acordos celebrados antes de 6 de maio de 2016, nomeadamente no domínio da aplicação do direito penal, e insta os Estados-Membros a determinar se é necessário uma maior harmonização com a legislação da UE em matéria de proteção de dados e com a jurisprudência.

O artigo 37.º da Diretiva Proteção de Dados na Aplicação da Lei também permite transferências internacionais de dados com base na autoavaliação por uma autoridade competente para determinar se um país terceiro (ou uma organização internacional) dispõe de garantias adequadas em matéria de proteção de dados. Nestes casos, a autoridade tem de documentar a transferência (nomeadamente, a sua data e hora, informações sobre a autoridade recetora, a justificação da transferência e os dados pessoais transferidos) e a documentação deve ser disponibilizada à autoridade de controlo a pedido desta (artigo 37.º, n.º 3, da Diretiva Proteção de Dados na

[170] Proposta de regulamento do Parlamento Europeu e do Conselho relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal, COM(2018) 225 final, e proposta de diretiva do Parlamento Europeu e do Conselho que estabelece normas harmonizadas aplicáveis à designação de representantes legais para efeitos de recolha de provas em processo penal, COM(2018) 226 final.

[171] CEPD, Declaração 2/2021 sobre o novo projeto de disposições do segundo protocolo adicional à Convenção do Conselho da Europa sobre o Cibercrime (Convenção de Budapeste), adotada em 2 de fevereiro de 2021, disponível em: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-022021-new-draft-provisions-second-additional_pt.

[172] Parecer da AEPD intitulado «Opinion 4/2021 on the Proposal for Amendment of the Europol Regulation» (não traduzido para português), adotado em 8 de março de 2021, disponível em: https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-proposal-amendment-europol-regulation_en.

[173] Declaração do CEPD intitulada «Statement 04/2021 on international agreements including transfers» (não traduzida para português), adotada em 13 de abril de 2021. Encontra-se disponível em: https://edpb.europa.eu/system/files/2021-04/edpb_statement042021_international_agreements_including_transfers_en.pdf.

Aplicação da Lei). As informações recebidas dos Estados-Membros[174] indicam que esta ferramenta raramente foi utilizada.

A fim de permitir que os Estados-Membros utilizem plenamente o conjunto de instrumentos de transferência da Diretiva Proteção de Dados na Aplicação da Lei, é importante que o CEPD intensifique os trabalhos que tem em curso sobre os vários mecanismos de transferência. Deve fornecer, entre outros, orientações sobre os mecanismos previstos no artigo 37.º, n.º 1, da Diretiva Proteção de Dados na Aplicação da Lei, nomeadamente sobre as transferências baseadas em autoavaliações por parte das autoridades competentes. O Conselho também sublinhou esta necessidade[175].

3.5.3 Utilização de derrogações

Por último, as chamadas «derrogações» constituem um motivo importante para as transferências em determinadas condições, previstas no artigo 38.º da Diretiva Proteção de Dados na Aplicação da Lei. Estas condições estabelecem um equilíbrio entre as considerações em matéria de privacidade e as necessidades operacionais das autoridades competentes. Em especial, o artigo 38.º, n.º 1, permite transferências, e mesmo categorias de transferências, de dados pessoais quando tal seja necessário para a prevenção de uma ameaça imediata e grave à segurança pública[176] ou, em casos individuais, para a prevenção, investigação, deteção ou repressão de infrações penais[177]. Contrariamente às derrogações ao abrigo do artigo 49.º do RGPD, não existem atualmente orientações para derrogações ao abrigo do artigo 38.º da Diretiva Proteção de Dados na Aplicação da Lei.

3.5.4 Cooperação policial e judiciária eficaz transnacional

A Diretiva Proteção de Dados na Aplicação da Lei tornou-se um ponto de referência internacional para a proteção de dados no contexto da aplicação da lei e funcionou como um catalisador para os países de todo o mundo ponderarem a introdução de regras modernas em matéria de privacidade neste domínio. Trata-se de uma evolução muito positiva, que proporciona novas oportunidades para proteger melhor as pessoas na UE quando os seus dados são transferidos para o estrangeiro

[174] Ver o relatório da Presidência do Conselho sobre o intercâmbio de dados policiais com países terceiros — Experiências na aplicação do artigo 37.º da Diretiva Proteção de Dados na Aplicação da Lei. O CEPD anunciou que incluirá as conclusões do relatório da Presidência, juntamente com mais informações e observações dos Estados-Membros, nos seus esforços para elaborar orientações sobre o artigo 37.º da diretiva. Ver a carta do presidente do CEPD à Representação Permanente da República Federal da Alemanha junto da União Europeia, de 26 de fevereiro de 2021 (documento 13555/1/20).
[175] Ver a posição do Conselho e conclusões sobre a aplicação da Diretiva Proteção de Dados na Aplicação da Lei, n.º 20.
[176] Artigo 38.º, n.º 1, alínea c), da Diretiva Proteção de Dados na Aplicação da Lei.
[177] Artigo 38.º, n.º 1, alínea d), da Diretiva Proteção de Dados na Aplicação da Lei.

para efeitos de aplicação da lei, facilitando simultaneamente os fluxos de dados que podem ajudar a combater a criminalidade.

Em termos mais gerais, é importante assegurar que as empresas ativas no mercado europeu, quando recebem pedidos de cooperação direta para partilhar dados para fins de aplicação da lei, possam fazê-lo sem terem de fazer face a conflitos de leis e no pleno respeito dos direitos fundamentais da UE[178]. A fim de melhorar esses tipos de transferências, a Comissão está empenhada em desenvolver quadros jurídicos adequados com os seus parceiros internacionais de modo a evitar conflitos de leis e a apoiar formas eficazes de cooperação, nomeadamente prevendo as necessárias garantias em matéria de proteção de dados, contribuindo assim para uma luta mais eficaz contra a criminalidade.

Face a esta realidade, a Comissão empenhou-se em promover ativamente, em contextos bilaterais, regionais e multilaterais, a convergência internacional das normas de proteção de dados para a cooperação em matéria de aplicação do direito penal. Durante os seus diálogos com vários países parceiros estrangeiros sobre as reformas em curso da legislação em matéria de proteção de dados, os serviços da Comissão empenharam-se de diferentes formas (por exemplo, contributos em resposta a consultas públicas, participação em audições parlamentares e reuniões específicas com representantes governamentais e decisores políticos) no desenvolvimento de regras sobre o tratamento de dados pessoais pelas autoridades competentes.

Num contexto regional e multilateral, a Comissão apoia, por exemplo, projetos de reforço das capacidades no contexto da aplicação da Convenção de Budapeste sobre o Cibercrime[179], do Conselho da Europa. Estes projetos incluem o programa GLACY +, destinado a reforçar a capacidade dos Estados para aplicarem a legislação em matéria de cibercriminalidade, bem como a sua capacidade para uma cooperação internacional eficaz, em conformidade com a Convenção de Budapeste e os seus protocolos adicionais. Tal implica também o desenvolvimento de legislação em matéria de proteção de dados para o tratamento de dados neste domínio. O programa apoia atualmente 17 países prioritários e centrais de África, Ásia-Pacífico, América Latina e Caraíbas.

A Comissão também colaborou com a Ameripol, uma organização de cooperação policial que reúne 18 países da América Latina, no contexto do desenvolvimento de um quadro de proteção de dados para o intercâmbio de informações entre a Ameripol e os seus Estados-Membros. Esta colaboração está a decorrer através de EL PAcCTO: Support to Ameripol, um projeto cujo objetivo é melhorar o nível de cooperação internacional entre os organismos policiais, judiciais e do Ministério Público dos países parceiros na luta contra a criminalidade organizada.

[178] A título de exemplo, o Segundo Protocolo Adicional à Convenção de Budapeste pode ser considerado um acordo internacional para efeitos do artigo 48.º do RGPD.
[179] Ver: https://www.coe.int/en/web/cybercrime/glacyplus.

A Comissão promove igualmente a Convenção 108 modernizada (conhecida como Convenção 108+)[180], que também é aplicável às atividades de tratamento de dados para efeitos de aplicação do direito penal. Esta Convenção, que está igualmente aberta a não membros do Conselho da Europa, é importante não só porque é o único acordo multilateral vinculativo em matéria de proteção de dados, mas também porque, através do seu Comité da Convenção, constitui um fórum para o intercâmbio de boas práticas e o estabelecimento de normas globais[181]. No âmbito da sua estratégia internacional em matéria de fluxos de dados, a Comissão incentiva a adesão de países terceiros à Convenção 108+.

Por último, a Comissão incentiva uma maior convergência a nível internacional, partilhando a nossa experiência com os parceiros sobre os aspetos da cooperação policial em matéria de proteção de dados. O «Instituto de Proteção de Dados» da Comissão, que faz parte do projeto «Cooperação Digital Internacional — Reforço da Proteção de Dados e dos Fluxos de Dados», financiado pelo Instrumento de Política Externa, é fundamental neste esforço. Este instituto foi criado para promover os intercâmbios entre reguladores europeus e de países terceiros e melhorar a cooperação no terreno. As atividades do instituto abrangem todos os aspetos da supervisão da proteção de dados, nomeadamente no domínio da aplicação da lei.

4 AÇÕES FUTURAS

A fim de assegurar uma política de segurança da UE eficiente que respeite plenamente o direito fundamental à proteção dos dados pessoais, a Comissão continuará a verificar se os Estados-Membros transpuseram corretamente a Diretiva Proteção de Dados na Aplicação da Lei e a controlar a aplicação das suas disposições.

A Diretiva Proteção de Dados na Aplicação da Lei contribuiu significativamente para um nível mais harmonizado e mais elevado de proteção dos direitos das pessoas e para um quadro jurídico mais coerente para as autoridades competentes.

De um modo geral, a Diretiva Proteção de Dados na Aplicação da Lei foi transposta de forma satisfatória, mas foram identificadas várias questões. A Comissão já deu início a procedimentos de infração relativos à não transposição e à não conformidade das legislações nacionais com a Diretiva Proteção de Dados na Aplicação da Lei. Continuará a trabalhar no sentido de assegurar uma transposição plena e correta.

---

[180] Protocolo de alteração da Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, adotado pelo Comité de Ministros na sua 128.ª sessão, em Elsinore, em 18 de maio de 2018 (Convenção 108+), disponível em: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[181] Ver, por exemplo, o «Practical guide on the use of personal data in the police sector» (um guia prático sobre a utilização de dados pessoais no setor da polícia), disponível em: https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5.

A Diretiva Proteção de Dados na Aplicação da Lei deu origem a um maior nível de sensibilização e atenção para a proteção de dados por parte das autoridades nacionais competentes, nomeadamente no que diz respeito à segurança do tratamento.

A supervisão ativa pelas autoridades de controlo da proteção de dados é fundamental para garantir que os objetivos da Diretiva Proteção de Dados na Aplicação da Lei são cumpridos na prática. Por conseguinte, é necessário dotar as autoridades de todos os tipos de poderes exigidos pela Diretiva Proteção de Dados na Aplicação da Lei, bem como de recursos adequados.

Nesta fase, a ênfase deve ser colocada na realização de todo o potencial da Diretiva Proteção de Dados na Aplicação da Lei. Neste contexto, e tendo em conta a experiência limitada com estas novas regras, a Comissão considera que é demasiado cedo para ponderar a revisão da Diretiva Proteção de Dados na Aplicação da Lei.

A Comissão continuará a trabalhar ativamente com todas as partes interessadas na perspetiva da próxima avaliação, prevista para 2026. Entretanto, continuará a trabalhar no sentido de assegurar a coerência com outra legislação da UE relevante para o tratamento de dados pessoais para efeitos de aplicação do direito penal.

Quadro jurídico

A Comissão pretende:

- continuar a avaliar a transposição da diretiva pelos Estados-Membros e tomar as medidas adequadas sempre que necessário (incluindo a instauração de procedimentos de infração),
- prosseguir os intercâmbios bilaterais com os Estados-Membros,
- assegurar que futuras propostas legislativas sejam coerentes com a Diretiva Proteção de Dados na Aplicação da Lei.

Os Estados-Membros devem:

- assegurar a transposição integral e correta da Diretiva Proteção de Dados na Aplicação da Lei a nível nacional, nomeadamente especificando os requisitos necessários da referida diretiva no caso de os atos nacionais de proteção de dados que a transpõem não o fazerem.

Supervisão pelas autoridades de controlo da proteção de dados

Os Estados-Membros devem:

- dotar as autoridades de controlo da proteção de dados de recursos suficientes para o desempenho das suas funções de aplicação da Diretiva Proteção de Dados na Aplicação da Lei,
- assegurar que as autoridades de controlo da proteção de dados possam exercer todos os tipos de poderes previstos na Diretiva Proteção de Dados na Aplicação da Lei,
- consultar sistematicamente as suas autoridades de controlo da proteção de dados sobre projetos legislativos e medidas administrativas de aplicação geral relacionados com a proteção de dados pessoais, e ter devidamente em conta os seus pareceres (especialmente no caso das novas tecnologias).

As autoridades de controlo da proteção de dados são convidadas a:

- utilizar plenamente os seus poderes de investigação, nomeadamente através da realização de inspeções por iniciativa própria,
- recolher estatísticas específicas relativas às suas atividades de supervisão no âmbito da Diretiva Proteção de Dados na Aplicação da Lei,
- utilizar os instrumentos de assistência mútua e desenvolver medidas práticas para facilitar os pedidos de assistência, nomeadamente através das orientações previstas do CEPD.

Convida-se o CEPD a:

- alargar a Reserva de Apoio de Peritos[182] para tarefas relacionadas com a Diretiva Proteção de Dados na Aplicação da Lei.

Apoio às autoridades competentes

A Comissão pretende:

- facilitar os debates e a partilha de experiências entre os Estados-Membros e a Comissão no âmbito do grupo de peritos dos Estados-Membros sobre a Diretiva Proteção de Dados na Aplicação da Lei,
- facilitar o intercâmbio de pontos de vista entre os responsáveis pela proteção de dados através da rede de responsáveis pela proteção de dados.

Os Estados-Membros são convidados a:

- prosseguir os esforços para realizar ações de formação sobre os requisitos em matéria de proteção de dados destinadas às autoridades competentes, nomeadamente no que diz respeito às novas tecnologias.

O CEPD e as autoridades de controlo da proteção de dados são convidados a:

- intensificar os seus esforços para adotar orientações pertinentes (por exemplo, sobre o papel do consentimento no contexto do tratamento de dados pessoais para efeitos de aplicação do direito penal e sobre os direitos dos titulares dos dados, incluindo as suas eventuais limitações), quer através da adoção de novas orientações autónomas, quer complementando as orientações já adotadas para o RGPD.

Transferências de dados transfronteiriças

A Comissão tenciona:

- promover ativamente eventuais novas decisões de adequação com os principais parceiros internacionais,
- negociar novos acordos de cooperação entre a Europol e a Eurojust, por um lado, e países terceiros, por outro. Se necessário, procurará renegociar os acordos de cooperação da Europol

[182] Documento do CEPD intitulado «Terms of Reference of the EDPB Support Pool of Experts» (não traduzido para português), adotado em 15 de dezembro de 2020.

em vigor, a fim de garantir que estes incluem garantias adequadas em matéria de proteção de dados,

- encetar negociações com o Japão com vista a alterar o atual Acordo de Auxílio Judiciário Mútuo UE-Japão, a fim de assegurar garantias adequadas em matéria de proteção de dados,
- prosseguir e concluir a negociação de um acordo bilateral com os Estados Unidos sobre o acesso transfronteiriço a provas eletrónicas para fins de cooperação judiciária em matéria penal, nomeadamente complementando as salvaguardas em matéria de proteção de dados garantidas pelo Acordo-Quadro UE-EUA, a fim de refletir o contexto específico da cooperação direta entre as autoridades responsáveis pela aplicação da lei e os prestadores de serviços,
- explorar a possibilidade de celebrar acordos-quadro de proteção de dados para o tratamento de dados no domínio da aplicação do direito penal com parceiros importantes no domínio da aplicação do direito penal, tomando como exemplo o Acordo-Quadro UE-EUA.

Convida-se o CEPD a:

- adotar orientações para clarificar melhor o conceito e o conteúdo das «salvaguardas adequadas» (artigo 37.º da Diretiva Proteção de Dados na Aplicação da Lei), bem como a utilização de derrogações (artigo 38.º da Diretiva Proteção de Dados na Aplicação da Lei).

Promover a convergência e desenvolver a cooperação internacional

A Comissão pretende:

- alargar o seu diálogo com os parceiros internacionais com vista a reforçar a convergência das regras de proteção de dados no domínio da aplicação do direito penal, nomeadamente promovendo a adesão à Convenção 108+ como único acordo mundial vinculativo em matéria de proteção de dados,
- promover a cooperação bilateral, regional e multilateral e apoiar projetos de reforço de capacidades no domínio da proteção de dados e da cooperação policial. Tal incluirá a formação e o intercâmbio de conhecimentos e de boas práticas através do Instituto de Proteção de Dados.

Os Estados-Membros são convidados a:

- ratificar rapidamente o Segundo Protocolo Adicional à Convenção de Budapeste do Conselho da Europa sobre o Cibercrime, logo que tal seja autorizado por uma decisão do Conselho.